```
File 350:Derwent WPIX 1963-2001/UD,UM &UP=200206
         (c) 2002 Derwent Info Ltd

Set     Items   Description
S1        413   FIREWALL? ? OR (BASTION OR PROXY)()HOST? ? OR APPLICATION(-
               )(GATEWAY? ? OR GUARD? ?)
S2      37937   TUNNEL? OR VIRTUAL()PRIVATE()CONNECT? OR VPN OR VPNS
S3     661915   AUTHENTICAT? OR VERIF? OR VALIDAT? OR IDENTIF? OR SCREEN???
              OR CHECK??? OR AUTHORIZ? OR AUTHORIS? OR PERMIT? OR PERMISSI-
              ON
S4      76634   SOCKET? ? OR WINSOCK OR SSL
S5    1047606   OBJECT? ? OR CLASS?? OR INHERITANCE OR JAVA OR APPLET? ? OR
              COMPONENT? ?
S6       8686   (CONFIGUR? OR TUNNEL?)(3N)(DATA OR INFORMATION) OR PORT? ?-
               (3N)(NUMBER? ? OR ADDRESS?? OR ID OR IDENTIF? OR IDENTIFICATI-
              ON) OR SESSION? ?(3N)(ID OR IDENTIF? OR IDENTIFICATION OR DATA
              OR INFORMATION) OR (SECURITY OR TUNNEL?)(5N)CONFIGUR?
S7          18  S1 AND S6
S8          18  S7 OR (S7 AND S2:S5)
S9          15  S1 AND S2
S10         15  S9 AND (S9 OR S3:S6)
S11         12  S10 NOT S8
S12        200  S2 AND S4
S13          2  S12 AND S6
S14          2  S13 NOT (S8 OR S11)
S15          8  S1 AND S4
S16          7  S15 NOT (S8 OR S11)
S17        197  S12 NOT (S8 OR S11 OR S13:S16)
S18          1  S17 AND IC=H04L
S19        208  VIRTUAL()PRIVATE()NETWORK?
S20          6  (S1 AND S19) NOT (S8 OR S11 OR S13:S16 OR S18)
S21          2  S19 AND S4
S22          2  S21 NOT (S8 OR S11 OR S13:S16 OR S18 OR S20)
S23          0  AU="BROWNELL D A":AU="BROWNELL D M" AND S1:S2
```

8/5/1
DIALOG(R)File 350:Derwent WPIX

014180644 **Image available**
WPI Acc No: 2002-001341/200201
Related WPI Acc No: 2001-572988; 2001-591651; 2001-597165; 2001-597166; 2001-598742
XRPX Acc No: N02-000996
Method and machine for configuring firewalls **in a computer data system**
Patent Assignee: BULL SA (SELA)
Inventor: FAVIER V; GRARDEL F; GUIONNEAU C
Number of Countries: 001 Number of Patents: 001
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
FR 2806812	A1	20010928	FR 9916121	A	19991221	200201	B

Priority Applications (No Type Date): FR 9916121 A 19991221
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
FR 2806812	A1		22	G06F-011/00	

Abstract (Basic): FR 2806812 A1
NOVELTY - Method of configuring a **firewall** (2) in a data system (3) having **objects** (4). An access control protocol is put in place for the **objects** being called by resources (13). Switching, for communication with the system, is controlled by imposing one or more network interfaces required for the passage of a communication between an origin resource and a destination resource.
DETAILED DESCRIPTION - Access to **firewall** protected zones (5) is not allowed to interfaces being used whilst the communication process is being done. Extended ownership services are used to allow the addition of supplementary switching application criteria. These criteria, as a function of which communication passage is imposed, are the calling address, the called address, the application called, the calling user, an **authentication** type, an application period (time and date of access), use level and/or an alert caused by a particular action associated with a particulate event.
An Independent Claim is included for - A **firewall** configuration machine.
USE - For access control to computer data systems
ADVANTAGE - Designed to allow a **firewall** administrator to control the switching of data packets at **firewall** level as a function of various criteria such as source **address** and/or **port numbers** , for a user who requests access at a particular time and date.
DESCRIPTION OF DRAWING(S) - The drawings shows a schematic of the **firewall** and system
configuration machine (1)
firewall (2)
data system (3)
objects (4)
firewall protected zones (5)
internal sub-network (6)
demilitarized sub network (7)
internet sub network (8)
liaison sub network for **firewalls** (9)
interfaces (10)
firewall configuration machine (11)
administrator (12)
resources (13)
graphical interface (14)
compilation driver (15)
tele-loading module (16)
pp; 22 DwgNo 1/3
Title Terms: METHOD; MACHINE; **FIREWALL** ; COMPUTER; DATA; SYSTEM
Derwent Class: T01; W01
International Patent Class (Main): G06F-011/00
International Patent Class (Additional): H04L-012/54

File Segment: EPI

8/5/2
DIALOG(R)File 350:Derwent WPIX

014131376 **Image available**
WPI Acc No: 2001-615587/200171
Related WPI Acc No: 2001-181126
XRPX Acc No: N01-459160
Information request managing method in computer network, involves selecting one or more of server systems to process information request based on examined configuration information
Patent Assignee: BMC SOFTWARE INC (BMCS-N)
Inventor: BRADDY R G
Number of Countries: 001 Number of Patents: 001
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
US 6304967	B1	20011016	US 97988107	A	19971210	200171	B
			US 2000596631	A	20000619		

Priority Applications (No Type Date): US 97988107 A 19971210; US 2000596631 A 20000619
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
US 6304967	B1		34	G06F-001/24	Cont of application US 97988107

Abstract (Basic): US 6304967 B1
NOVELTY - When a request is made by a client computer (42,44,48), the workloads associated with the first and second servers (72,74) are determined and the one with the lightest workload is deals with the request. A list is kept of all the processes that can be carried out by each server so that it does not have to deal with requests it can't handle. When workloads are the same, requests are distributed in a round-robin fashion.
DETAILED DESCRIPTION - INDEPENDENT CLAIMS are included for (1) A computer readable medium with a program for managing data requests.
(2) A system for managing data requests.
USE - Distributing, monitoring and managing information requests across a distributed computing environment.
ADVANTAGE - Deals with problems of depletion of computing ability from use of interactivity like CGI scripts, **firewall** bottlenecking and lack of network management tools.
DESCRIPTION OF DRAWING(S) - The drawing shows a computer network configured as the invention.
pp; 34 DwgNo 4/18
Title Terms: INFORMATION; REQUEST; MANAGE; METHOD; COMPUTER; NETWORK; SELECT; ONE; MORE; SERVE; SYSTEM; PROCESS; INFORMATION; REQUEST; BASED; CONFIGURATION; INFORMATION
Derwent Class: T01
International Patent Class (Main): G06F-001/24
File Segment: EPI

8/5/3
DIALOG(R)File 350:Derwent WPIX

014107521 **Image available**
WPI Acc No: 2001-591733/200167
XRPX Acc No: N01-440925
Method and machine for centralized configuration of firewall **in TCP/IP internet protocol data system, system description specification is separated from access control policy in form of access rule between origin and destination resources**
Patent Assignee: BULL SA (SELA)
Inventor: FAVIER V; GRARDEL F; GUIONNEAU C; SOINNE F

Number of Countries: 001 Number of Patents: 001
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
FR 2802662	A1	20010622	FR 9916120	A	19991221	200167	B

Priority Applications (No Type Date): FR 9916120 A 19991221
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
FR 2802662	A1		34	G06F-011/00	

Abstract (Basic): FR 2802662 A1
NOVELTY - The method has:
(a) a description stage for each resource (7) of the data system (3), via a graphical and data collector interface (8);a description stage, via the graphical and data collector interface, for an access control rule, between a origin resource and a destination resource, allowing definition of an access control policy between the two resources;the two stages are realized in an independent manner
DETAILED DESCRIPTION - The **firewall** (2) **configuration** device, for a **data** system (3) includes a central configuration machine (5) having (a) a graphical interface (8) describing the system and access control policy to the resources (7); (b) a compilation motor (9) which translates the collected data from the interface (8) in access control rules; (c) a teleloading and synchronizing module (10) designed to ensure transfer, of the rules created by the motor (9), to the appropriate **firewall** . The module (10) communicates with the group of **firewalls** , at the instant which the new transferred rule files are taken into account and applied.
USE - For centralized configuration of **firewalls** in a internet network.
ADVANTAGE - Designed to simplify the configuration of a large number of **firewalls** .
DESCRIPTION OF DRAWING(S) - The drawing shows a schematic diagram of one version of the system
firewalls (2)
system (3)
central configuration machine (5)
administrator (6)
resources (7)
graphical interface (8)
compilation motor (9)
teleloading and synchronizing module (10)
sub-network enclosure zones (15)
pp; 34 DwgNo 1/5
Title Terms: METHOD; MACHINE; CONFIGURATION; **FIREWALL** ; IP; PROTOCOL; DATA ; SYSTEM; SYSTEM; DESCRIBE; SPECIFICATION; SEPARATE; ACCESS; CONTROL; FORM; ACCESS; RULE; ORIGIN; DESTINATION; RESOURCE
Derwent Class: T01; W01
International Patent Class (Main): G06F-011/00
International Patent Class (Additional): G06F-015/177; H04L-012/66
File Segment: EPI

8/5/4
DIALOG(R)File 350:Derwent WPIX

013940108 **Image available**
WPI Acc No: 2001-424322/200145
Related WPI Acc No: 2001-307248
XRPX Acc No: N01-314717
Network security **device reconfiguration involves copying** configuration data **of** security **device from directory location to sub-directory and other low level sub-directory directly or indirectly coupled to sub-directory**
Patent Assignee: ANTUR A K (ANTU-I); BISHT N S (BISH-I); PURI H (PURI-I); SAWHNEY S (SAWH-I)
Inventor: ANTUR A K; BISHT N S; PURI H; SAWHNEY S

Number of Countries: 001 Number of Patents: 001
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
US 6243815	B1	20010605	US 9744853	A	19970425	200145	B
			US 97998313	A	19971224		

Priority Applications (No Type Date): US 9744853 P 19970425; US 97998313 A 19971224
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
US 6243815	B1		19	G06F-011/00	Provisional application US 9744853

Abstract (Basic): US 6243815 B1

NOVELTY - Hierarchical directory structure having interconnected sub-directories is provided. **Configuration data** for network **security** devices is stored at predetermined directory location and copied to primary sub-directory in response to primary reconfigure request. **Configuration data** from sub-directory is copied to a low level sub-directory directly or indirectly coupled to primary sub-directory and installed on any network **security** device. Configuration of network **security** devices are updated based on **configuration data** .

DETAILED DESCRIPTION - INDEPENDENT CLAIMS are also included for the following:

(a) Network **security** device **configuring** method;

(b) Network of security devices

USE - For managing multi-platform **firewalls** , during accessing of internet.

ADVANTAGE - Enables **firewalls** to work in hybrid network environments that employ multiple protocols and multiple platforms.

DESCRIPTION OF DRAWING(S) - The figure shows the schematic diagram of system for reconfiguring and managing network security devices.

pp; 19 DwgNo 2/6

Title Terms: NETWORK; SECURE; DEVICE; RECONFIGURE; COPY; CONFIGURATION; DATA; SECURE; DEVICE; DIRECTORY; LOCATE; SUB; DIRECTORY; LOW; LEVEL; SUB; DIRECTORY; INDIRECT; COUPLE; SUB; DIRECTORY
Derwent Class: T01
International Patent Class (Main): G06F-011/00
File Segment: EPI

8/5/5

013823036 **Image available**
WPI Acc No: 2001-307248/200132
Related WPI Acc No: 2001-424322
XRPX Acc No: N01-219807

Network security **devices** configuring **method e.g. for multiplatform** firewalls , **involves implementing security policy for** security **devices and providing** configuration information **for devices**

Patent Assignee: ANTUR A K (ANTU-I); BISHT N S (BISH-I); PURI H (PURI-I); SAWHNEY S (SAWH-I)
Inventor: ANTUR A K; BISHT N S; PURI H; SAWHNEY S
Number of Countries: 001 Number of Patents: 001
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
US 6212558	B1	20010403	US 9744853	A	19970425	200132	B
			US 97998100	A	19971224		

Priority Applications (No Type Date): US 9744853 P 19970425; US 97998100 A 19971224
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
US 6212558	B1		35	G06F-015/16	Provisional application US 9744853

Abstract (Basic): US 6212558 B1

NOVELTY - A network directory services server provides network directory services to the network connecting network security devices such as multilevel IP **firewall** and IPX/IP gateway. A database in the server, stores network **configuration information** . A **security** policy is implemented for the **security** devices, based on which **configuration information** is provided to devices and stored in database.

DETAILED DESCRIPTION - INDEPENDENT CLAIMS are also included for the following:

(a) Method of **configuring security** features in networks;

(b) Network of trusted network servers

USE - For configuring multiplatform **firewalls** used to control access between private trusted network and untrusted network such as internet or corporate network within intranet.

ADVANTAGE - Combines capabilities of packet filter, circuit level gateway and application level gateway to provide in-depth defense. Provides enhanced security and support for multiprotocol networks by integrating multilevel IP **firewall** and IPX/IP gateway.

DESCRIPTION OF DRAWING(S) - The figure shows the **security** devices **configuring** system.

pp; 35 DwgNo 2/25

Title Terms: NETWORK; SECURE; DEVICE; METHOD; **FIREWALL** ; IMPLEMENT; SECURE ; SECURE; DEVICE; CONFIGURATION; INFORMATION; DEVICE

Derwent Class: T01

International Patent Class (Main): G06F-015/16

File Segment: EPI

8/5/6

DIALOG(R)File 350:Derwent WPIX

013759817 **Image available**

WPI Acc No: 2001-244029/200125

Related WPI Acc No: 2000-270565; 2000-375616

XRPX Acc No: N01-173747

Configuration management interface in multiserver for providing integrated computer services, has definition screens **to display configuration of computer services and to allow administrator to define characteristics**

Patent Assignee: NTK.COM CORP (NTKC-N)

Inventor: BAULCH J; BONI B; DICK A; KIRCHKNOPF J

Number of Countries: 092 Number of Patents: 002

Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
WO 200060451	A2	20001012	WO 2000CA348	A	20000331	200125	B
AU 200035475	A	20001023	AU 200035475	A	20000331	200125	

Priority Applications (No Type Date): US 99127609 P 19990401

Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
WO 200060451	A2	E	103	G06F-009/00	

Designated States (National): AE AG AL AM AT AU AZ BA BB BG BR BY CA CH CN CR CU CZ DE DK DM DZ EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT TZ UA UG US UZ VN YU ZA ZW

Designated States (Regional): AT BE CH CY DE DK EA ES FI FR GB GH GM GR IE IT KE LS LU MC MW NL OA PT SD SE SL SZ TZ UG ZW

AU 200035475	A		G06F-009/00	Based on patent WO 200060451

Abstract (Basic): WO 200060451 A2

NOVELTY - The configuration definition unit has configuration definition **screens** for displaying the configuration of computer services and for allowing the administrator to define the characteristics. The configuration implementation unit configures several computer services to correspond to the characteristics.

DETAILED DESCRIPTION - The locking unit ensures that one of the characteristics can be defined only by the administrator, and

selectively restricts access to one of the configuration definition **screens** . The operation of **firewall** installed on computer is controlled by the administrator. The relationship between each of servers and **firewall** is indicated by displaying elements relating to each of servers on the configuration definition **screens** in one or more selected colors. INDEPENDENT CLAIMS are also included for the following:

(a) multiserver;

(b) facsimile transmission processing method;

(c) method of relaying piece of electronic mail transmitted from transmitting computer to receiving computer through host computer

USE - In multiserver for providing integrated computer services such as file sharing service, print services, e-mail services, security service, facsimile services and internet hosting services, required by business enterprise, etc. Also for providing word processing, spreadsheet, internet, and home automation and networking services.

ADVANTAGE - The configuration management interface automatically configures the underlying packages in response to information entered by the administrator, by allowing the administrator to enter all **data** required to **configure** each server in single environment. The underlying software packages can be changed without changing the appearance of configuration management interface, allowing the system to be upgraded without requiring the administrator to learn how to configure new packages. Allows the multiserver to be improved and modified in a manner transparent to administrator and other users of system thereby reduces the need for highly qualified technical personnel to configure and operate the multiserver.

DESCRIPTION OF DRAWING(S) - The figure shows the block diagram explaining interconnections between elements of multiserver.

pp; 103 DwgNo 1/19

Title Terms: CONFIGURATION; MANAGEMENT; INTERFACE; INTEGRATE; COMPUTER; SERVICE; DEFINE; **SCREEN** ; DISPLAY; CONFIGURATION; COMPUTER; SERVICE; ALLOW; ADMINISTER; DEFINE; CHARACTERISTIC

Derwent Class: T01; W01; W02

International Patent Class (Main): G06F-009/00

File Segment: EPI

8/5/7

DIALOG(R)File 350:Derwent WPIX

013696902 **Image available**

WPI Acc No: 2001-181126/200118

Related WPI Acc No: 2001-615587

XRPX Acc No: N01-129067

Information request managing method in computer network, involves selecting one or more of server systems to process information request based on examined configuration information

Patent Assignee: BMC SOFTWARE INC (BMCS-N)

Inventor: BRADDY R G

Number of Countries: 001 Number of Patents: 001

Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
US 6141759	A	20001031	US 97988107	A	19971210	200118	B

Priority Applications (No Type Date): US 97988107 A 19971210

Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
US 6141759	A		50	G06F-017/50	

Abstract (Basic): US 6141759 A

NOVELTY - **Configuration information** relative to resources available on server systems and relative to types of information requests received by initial server, is examined to determine if one or more of other systems are capable of processing requests. At least one of systems are selected to process information to distribute requests received by initial server among selected one of server based on

determination.

DETAILED DESCRIPTION - Information request from the client computer system is received at initial server computer system. The **configuration information** is examined to determine whether the received information request corresponds to one of information request types to be managed by the initial server system, based on which information request to be processed on either of the server systems is determined. The information request is processed on the selected server system and the results are transmitted to the client computer system. INDEPENDENT CLAIMS are also included for the following:

(a) secure information distribution method;

(b) network enterprise management system;

(c) information request distribution program

USE - For distributing, monitoring and managing information requests across distributed computing environment or computer network such as internet, intranet.

ADVANTAGE - Provides for monitoring and fault recovery for information requests received by server computer system. Provides limited and secure access to information and application on server computer system protected by network **firewall** .

DESCRIPTION OF DRAWING(S) - The figure shows the diagram of computer network.

pp; 50 DwgNo 4/18

Title Terms: INFORMATION; REQUEST; MANAGE; METHOD; COMPUTER; NETWORK; SELECT; ONE; MORE; SERVE; SYSTEM; PROCESS; INFORMATION; REQUEST; BASED; CONFIGURATION; INFORMATION

Derwent Class: T01

International Patent Class (Main): G06F-017/50

File Segment: EPI

8/5/8

DIALOG(R)File 350:Derwent WPIX

013605690 **Image available**

WPI Acc No: 2001-089898/200110

XRPX Acc No: N01-068052

Information communication apparatus for internet system, adjusts transmission rate of information package in preset time interval between user and network ports with respect to bandwidth allocated to each user port

Patent Assignee: BBN CORP (BBNB-N)

Inventor: JOFFE R L; OBENHUBER T

Number of Countries: 001 Number of Patents: 001

Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
US 6144638	A	20001107	US 9619089	A	19960514	200110	B
			US 97853862	A	19970509		

Priority Applications (No Type Date): US 9619089 P 19960514; US 97853862 A 19970509

Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
US 6144638	A		19	H04L-012/56	Provisional application US 9619089

Abstract (Basic): US 6144638 A

NOVELTY - A controller regulates the transmission of the information packets between a user port and a network port in a preset time interval based on the bandwidth allocated to the user port. **Firewalls** (470-473) filter the network traffic to the user port corresponding to the security features of the user port.

DETAILED DESCRIPTION - The bandwidth and the security features allocated to each user port is contained in a **configuration information** stored in a non-volatile computer memory. A switch establishes a communication path between a user port and a network port. An INDEPENDENT CLAIM is also included for a data distribution method in internet system.

USE - In internet system.

ADVANTAGE - Enables to specify bandwidth for each user port. Enables to monitor software and control functions. Provides a dedicated service at a lower operational cost. Reduces entry cost for internet connection. Provides high capacity connection at a low cost. Provides completely integrated internet hook-up service.

DESCRIPTION OF DRAWING(S) - The figure shows the functional block diagram of communication apparatus.

Firewalls (470-473)

pp; 19 DwgNo 4/8

Title Terms: INFORMATION; COMMUNICATE; APPARATUS; SYSTEM; ADJUST; TRANSMISSION; RATE; INFORMATION; PACKAGE; PRESET; TIME; INTERVAL; USER; NETWORK; PORT; RESPECT; BANDWIDTH; ALLOCATE; USER; PORT

Derwent Class: T01; W01

International Patent Class (Main): H04L-012/56

File Segment: EPI

8/5/9

DIALOG(R)File 350:Derwent WPIX

013564709 **Image available**

WPI Acc No: 2001-048916/200106

XRPX Acc No: N01-037460

Physical layer circuit arrangement for interfacing local node in electronic device to memory-mapped serial communications interface has security manager coupled to link layer interface and configured **to modify** data **packet**

Patent Assignee: VLSI TECHNOLOGY INC (VLSI-N)

Inventor: CORNELIUS S; LEVY P S

Number of Countries: 001 Number of Patents: 001

Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
US 6134662	A	20001017	US 98105553	A	19980626	200106	B

Priority Applications (No Type Date): US 98105553 A 19980626

Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
US 6134662	A		31	G06F-012/14	

Abstract (Basic): US 6134662 A

NOVELTY - A link layer interface configured to transmit and receive data from the link layer. A security manager (26,28) is coupled to the link layer interface and **configured** to modify a **data** packet which has a **checksum** , received over the interface from an unauthorized node. The link layer discards of data packets having an invalid **checksum** .

DETAILED DESCRIPTION - The **security** manager (26,28) is **configured** to modify the **data** packet by modifying the **checksum** . The **security** manager is also **configured** to transmit an acknowledgement over the communications interface to the unauthorized node, which indicates that data requested by the unauthorized node is unavailable.

INDEPENDENT CLAIMS are included for the following; A method of controlling access to a local node in an electronic device from a memory mapped serial communications interface of the type that supports peer-to-peer communications between a number of nodes, and A method of implementing secure communications over a memory-mapped serial communications interface of the type that supports unsecured peer-to-peer communications between a number of nodes.

USE - For interfacing a local node in an electronic device to a memory-mapped serial communications interface.

ADVANTAGE - Securing data communication over a memory-mapped communications interface and comparability is retained with existing standard, and does not require significant additional expenditure and effort. Secure data transmission between devices over an IEEE 1394-based interface while retaining compatibility with legacy IEEE 1394-compatible devices coupled to such an interface is supported.

DESCRIPTION OF DRAWING(S) - The figure shows a block diagram of a data processing system implementing a distributed fire wall.
Communications interface (10)
Number of nodes (12,14,16,18,20,22)
Security managers (26,28)
pp; 31 DwgNo 1/17
Title Terms: PHYSICAL; LAYER; CIRCUIT; ARRANGE; INTERFACE; LOCAL; NODE; ELECTRONIC; DEVICE; MEMORY; MAP; SERIAL; COMMUNICATE; INTERFACE; SECURE; MANAGE; COUPLE; LINK; LAYER; INTERFACE; CONFIGURATION; MODIFIED; DATA; PACKET
Derwent Class: T01; W01
International Patent Class (Main): G06F-012/14
File Segment: EPI

8/5/10

DIALOG(R)File 350:Derwent WPIX

013557795 **Image available**
WPI Acc No: 2001-042002/200106
XRPX Acc No: N01-031438
Server input control unit prevents Denial of Service attacks
Patent Assignee: WITTKOETTER E (WITT-I)
Number of Countries: 001 Number of Patents: 001
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
DE 20004355	U1	20000824	DE 2000U2004355	U	20000310	200106	B

Priority Applications (No Type Date): DE 2000U2004355 U 20000310
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
DE 20004355	U1		19	H04L-009/00	

Abstract (Basic): DE 20004355 U1
NOVELTY - The input control unit (24) controlled by the input control server (26) is outside the **firewall** (20) and allocates **session identification** parameters to clients (14,16,18) detected by the test unit (22) so that multiple connection attempts can be rejected.
USE - Protection of internet servers from Denial of Service attacks.
ADVANTAGE - Both Denial of Service and Distributed Denial of Service attacks are prevented. The control server and test unit cannot be subjected to complex requests and so are less vulnerable than the server which they protect.
DESCRIPTION OF DRAWING(S) - The drawing is a block diagram of the system.
Server (10)
Internet (12)
Clients (14,16,18)
Firewall unit (20)
Test unit (22)
Input control unit (24)
Input control server (26)
pp; 19 DwgNo 1/1
Title Terms: SERVE; INPUT; CONTROL; UNIT; PREVENT; SERVICE; ATTACK
Derwent Class: W01
International Patent Class (Main): H04L-009/00
International Patent Class (Additional): H04L-012/22
File Segment: EPI

8/5/11

DIALOG(R)File 350:Derwent WPIX

013378896 **Image available**

WPI Acc No: 2000-550834/200051
XRPX Acc No: N00-407510
Apparatus to manage a firewall **providing important safeguards to any network connected to the Internet by facilitating generation of a security policy**
Patent Assignee: LUCENT TECHNOLOGIES INC (LUCE)
Inventor: BARTAL Y; MAYER A J; WOOL A
Number of Countries: 027 Number of Patents: 003
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
EP 1024627	A2	20000802	EP 2000300371	A	20000119	200051	B
CA 2296989	A1	20000729	CA 2296989	A	20000118	200051	
JP 2000253066	A	20000914	JP 200019884	A	20000128	200053	

Priority Applications (No Type Date): US 99240934 A 19990129
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
EP 1024627	A2	E	23	H04L-012/24	
Designated States (Regional): AL AT BE CH CY DE DK ES FI FR GB GR IE IT LI LT LU LV MC MK NL PT RO SE SI					
CA 2296989	A1	E		H04L-029/06	
JP 2000253066	A		19	H04L-012/56	

Abstract (Basic): EP 1024627 A2
NOVELTY - An internal **firewall** (150) behind a server zone (130) guards the corporation proprietary or internal network and has three interfaces, one to the server zone, a second to a corporate network zone (160) and a third to an administration zone (140). An external **firewall** (120) guards the connection to an external network and the **firewalls** each have a packet filtering configuration file (125,155), while a **firewall** manager (200) allows a security policy to be generated for a network environment (100) and automatically generates **firewall** -specific **configuration** files from the **security** policy simultaneously for multiple gateways.
DETAILED DESCRIPTION - INDEPENDENT CLAIMS are included for a method of generating a configuration file for a network, for a method and parser for producing an entity-relationship model of a security policy, for a security policy generating system and for a configuration file compiler.
USE - Managing a **firewall** in a network connection to the Internet.
ADVANTAGE - Automatically generating rule-bases from security policy.
DESCRIPTION OF DRAWING(S) - The drawing illustrates a representative network environment according to the present invention
Internal and external **firewalls** (120,150)
Server, corporate network and administration zones (130,160,140)
Filtering configuration files (125,155)
Firewall manager (200)
pp; 23 DwgNo 1/9
Title Terms: APPARATUS; MANAGE; **FIREWALL** ; IMPORTANT; SAFEGUARD; NETWORK; CONNECT; FACILITATE; GENERATE; SECURE
Derwent Class: W01
International Patent Class (Main): H04L-012/24; H04L-012/56; H04L-029/06
International Patent Class (Additional): G06F-013/00; H04L-012/22; H04L-012/26; H04L-012/28; H04L-012/46; H04L-012/66
File Segment: EPI

8/5/12
DIALOG(R)File 350:Derwent WPIX

013377112 **Image available**
WPI Acc No: 2000-549050/200050
XRPX Acc No: N00-406191
Internet protocol key management mechanism for internet security architecture, has index pointers to point index to identify session

keys whose divergence barrier is unbarred by unbar data sets

Patent Assignee: METEORA SYSTEM KK (METE-N); WATANABE E (WATA-I)
Inventor: SEKIGUCHI Y; TAKE H; TOJIMA Y; WATANABE E; YAMADA T
Number of Countries: 021 Number of Patents: 002
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
WO 200046967	A1	20000810	WO 99JP476	A	19990204	200050	B
EP 1068711	A1	20010117	EP 99973672	A	19990204	200105	
			WO 99JP476	A	19990204		

Priority Applications (No Type Date): WO 99JP476 A 19990204
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
WO 200046967	A1	E	26	H04L-029/06	

Designated States (National): JP US
Designated States (Regional): AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE

EP 1068711	A1	E		H04L-029/06	Based on patent WO 200046967

Designated States (Regional): AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE

Abstract (Basic): WO 200046967 A1

NOVELTY - Key generators (51,61) generate session keys (53,63) indexed for **identification** from IP key (11) for entering closed IP network. The session keys include divergence barrier for barring computational approach to an arbitrary session key. Index pointers (71,72) point index (i,j) to **identify session** keys. Unbar **data** sets unbar the divergence barrier.

DETAILED DESCRIPTION - The **session** keys are **information** -theoretically isolated from each other by drop of information having corresponding entropy difference. The entropy difference is developed along the way of computational approach by the divergence barrier. The divergence barrier comprises tree of candidate keys for arbitrary session key. The tree of candidate keys divergence with increasing number of candidate keys beyond computationally secure number as the computational approach makes way. The unbar data set includes regenerated set of session keys and sequence of index combinations for **identifying** unique **session** key.

USE - For internet security architecture such as IPSEC.

ADVANTAGE - A used session key can be fetched and a computational approach can be tried in forward and backward senses of temporal direction of key selection. The unbar data set unveils the set of session keys to associated peers thereby allowing IP inline security service for peers. The index pointer points index to **identify session** key which is used or to be used in network thereby **permitting** voluntary key selection which is independent of key generation order. **Permits** long term security service of original keying material, thereby supporting perfect secrecy of session keys and IP inline security service which is free from frequent interruptions via out-of-band mechanisms. Provides virtual private networks (**VPNs**) whose security services support perfect secrecy for session keys at reduced cost and also provides unconditional security for original keying material even to manual keying. Allows long-term service of keying material for IP-layer thereby **permitting** manually configured keying for selective encryption of **firewall** . Contributes to business-to-business **tunneling** protocol without certificate authorities.

DESCRIPTION OF DRAWING(S) - The figure shows block diagram of IP key management mechanism.

IP key (11)
Key generators (51,61)
Session keys (53,63)
Index pointers (71,72)
pp; 26 DwgNo 2/8

Title Terms: PROTOCOL; KEY; MANAGEMENT; MECHANISM; SECURE; ARCHITECTURE; INDEX; POINT; POINT; INDEX; **IDENTIFY** ; SESSION; KEY; DIVERGE; BARRIER; DATA; SET
Derwent Class: W01

International Patent Class (Main): H04L-029/06
International Patent Class (Additional): H04L-009/08
File Segment: EPI

8/5/13
DIALOG(R)File 350:Derwent WPIX

012815569 **Image available**
WPI Acc No: 1999-621800/199954
XRPX Acc No: N99-458802
Computer security apparatus e.g. for firewall **security technique employed in computer networks**
Patent Assignee: LUCENT TECHNOLOGIES INC (LUCE)
Inventor: CHESWICK W R; WHITTEN E G
Number of Countries: 030 Number of Patents: 006
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
EP 952715	A2	19991027	EP 99302021	A	19990316	199954	B
CA 2261553	A1	19990924	CA 2261553	A	19990210	200008	
JP 11353258	A	19991224	JP 9979042	A	19990324	200011	
KR 99078198	A	19991025	KR 9910002	A	19990324	200052	
US 1944	H	20010206	US 9847207	A	19980324	200109	
TW 414876	A	20001211	TW 99101536	A	19990202	200124	

Priority Applications (No Type Date): US 9847207 A 19980324
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
EP 952715	A2	E	13	H04L-029/06	
Designated States (Regional): AL AT BE CH CY DE DK ES FI FR GB GR IE IT LI LT LU LV MC MK NL PT RO SE SI					
CA 2261553	A1	E		H04L-009/32	
JP 11353258	A		11	G06F-013/00	
KR 99078198	A			G06F-015/17	
US 1944	H			G06F-012/14	
TW 414876	A			G06F-013/00	

Abstract (Basic): EP 952715 A2
NOVELTY - The apparatus has a memory which stores several security routines, the number of security routines defines at least one security requirement. A connector connects the computer security apparatus to a user terminal. A processor applies one security routine to a communications stream of the user terminal, a portion of the communications stream is transmitted through the computer security apparatus. The communications stream is received by the user terminal from a public network.
DETAILED DESCRIPTION - An INDEPENDENT CLAIM is include for a dongle for providing a client based **firewall** , a client based **firewall** system, a method for providing a client based **firewall** , and a computer network security method.
USE - For **firewall** security technique employed in computer networks.
ADVANTAGE - Provides client based **firewall** technique which provides for network security within private network.
DESCRIPTION OF DRAWING(S) - The figure shows an illustrative **firewall** **security** device **configured** in accordance with the principles of the invention.
pp; 13 DwgNo 2/6
Title Terms: COMPUTER; SECURE; APPARATUS; **FIREWALL** ; SECURE; TECHNIQUE; EMPLOY; COMPUTER; NETWORK
Derwent Class: W01
International Patent Class (Main): G06F-012/14; G06F-013/00; G06F-015/17; H04L-009/32; H04L-029/06
International Patent Class (Additional): H04L-012/22; H04L-012/56
File Segment: EPI

8/5/14
DIALOG(R)File 350:Derwent WPIX

012422946 **Image available**
WPI Acc No: 1999-229054/199919
XRPX Acc No: N99-169497
Data communication system using port number **and IP** address
Patent Assignee: TELEFONAKTIEBOLAGET ERICSSON L M (TELF)
Inventor: NILSEN B
Number of Countries: 082 Number of Patents: 004
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
WO 9912298	A2	19990311	WO 98NO239	A	19980814	199919	B
NO 9704028	A	19990303	NO 974028	A	19970902	199919	
NO 305420	B1	19990525	NO 974028	A	19970902	199927	
AU 9888205	A	19990322	AU 9888205	A	19980814	199931	

Priority Applications (No Type Date): NO 974028 A 19970902
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
WO 9912298	A2	E	20	H04L-000/00	
NO 305420	B1			H04L-029/06	Previous Publ. patent NO 9704028
AU 9888205	A			H04L-000/00	Based on patent WO 9912298
NO 9704028	A			H04L-029/06	

Designated States (National): AL AM AT AU AZ BA BB BG BR BY CA CH CN CU CZ DE DK EE ES FI GB GE GH GM HR HU ID IL IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MD MG MK MN MW MX NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT UA UG US UZ VN YU ZW
Designated States (Regional): AT BE CH CY DE DK EA ES FI FR GB GH GM GR IE IT KE LS LU MC MW NL OA PT SD SE SZ UG ZW

Abstract (Basic): WO 9912298 A2
NOVELTY - Uses data communication system where users, managers or machines intercommunicate via **ports** with **port number** and Internet Protocol address using classification and logic for ports to communicate via **firewalls** (fig 1). Includes a **bastion host** that accepts digitally signed configuration messages from distributed operators and managers to ensure the integrity of the messages.
USE - For protecting applications utilizing dynamic port allocation.
ADVANTAGE - Substantially improves security issues.
DESCRIPTION OF DRAWING(S) - The drawing shows schematic block diagram illustrating a basic **firewall** architecture with its main elements.
basic **firewall** (fig 1)
pp; 20 DwgNo 1/2
Title Terms: DATA; COMMUNICATE; SYSTEM; PORT; NUMBER; IP; ADDRESS
Derwent Class: T01; W01
International Patent Class (Main): H04L-000/00; H04L-029/06
File Segment: EPI

8/5/15
DIALOG(R)File 350:Derwent WPIX

012411203 **Image available**
WPI Acc No: 1999-217311/199919
XRPX Acc No: N99-160200
Computer network firewall **packet** validation
Patent Assignee: LUCENT TECHNOLOGIES INC (LUCE)
Inventor: COSS M J; MAJETTE D L; SHARP R L
Number of Countries: 027 Number of Patents: 003
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
EP 909072	A2	19990414	EP 98306984	A	19980901	199919	B
JP 11163940	A	19990618	JP 98252831	A	19980907	199935	

US 6141749 A 20001031 US 97928794 A 19970912 200057

Priority Applications (No Type Date): US 97928794 A 19970912
Patent Details:
Patent No Kind Lan Pg Main IPC Filing Notes
EP 909072 A2 E 21 H04L-029/06
Designated States (Regional): AL AT BE CH CY DE DK ES FI FR GB GR IE IT LI LT LU LV MC MK NL PT RO SE SI
JP 11163940 A 18 H04L-012/56
US 6141749 A H04L-009/14

Abstract (Basic): EP 909072 A2
NOVELTY - The method involves storing in a cache a result of applying at least a portion of a rule set to a given packet of a network session. The stored results are used to process at least one subsequent packet having a characteristic similar to that of the given packet.
DETAILED DESCRIPTION - The cache can include a **session** key, hardware address **information** , interface information, number of an applicable rule, alarm code, statistical information, and an applicable action. The session key includes at least one header item which was appended to the data to be transmitted in the packet; it may include the Internet protocol (IP) source address, the IP destination address, a next-level protocol, e.g. transmission control protocol (TCP), or universal datagram protocol (UDP), a source port associated with the protocol, and the destination port associated with the protocol.
An INDEPENDENT CLAIM is included for an apparatus for use in **validating** a packet in a **firewall** of a computer network.
USE - For preventing unauthorized access to computer networks using **firewall** protection.
ADVANTAGE - Improves processing efficiency; improves security; increase access rule flexibility, and enhances ability of **firewall** to deal with complex protocols.
DESCRIPTION OF DRAWING(S) - The drawing is a flow chart of dependency of mask processing.
pp; 21 DwgNo 9/10
Title Terms: COMPUTER; NETWORK; **FIREWALL** ; PACKET; VALID
Derwent Class: W01
International Patent Class (Main): H04L-009/14; H04L-012/56; H04L-029/06
International Patent Class (Additional): G06F-013/00; H04L-012/28; H04L-012/46; H04L-012/66
File Segment: EPI

8/5/16
DIALOG(R)File 350:Derwent WPIX

012166119 **Image available**
WPI Acc No: 1998-583031/199849
Related WPI Acc No: 2000-375433
XRPX Acc No: N98-454261
Fire wall system for protecting network components **e.g. router, server, database, hosts, modem - uses proxy agent to** verify **authority of incoming call, by** checking **whether time period during which incoming access request is received, is valid**
Patent Assignee: NETWORK ENG SOFTWARE (NETW-N)
Inventor: COLEY C D; WESINGER R E
Number of Countries: 001 Number of Patents: 001
Patent Family:
Patent No Kind Date Applicat No Kind Date Week
US 5826014 A 19981020 US 96595957 A 19960206 199849 B

Priority Applications (No Type Date): US 96595957 A 19960206
Patent Details:
Patent No Kind Lan Pg Main IPC Filing Notes
US 5826014 A 15 G06F-012/14

Abstract (Basic): US 5826014 A

The system includes a fire wall box comprising a stand along computing platform. A connector is used for interconnecting **firewall** box to network **components** . A proxy agent is assigned to incoming request, in accordance with **port number** .

The proxy agent **verifies** the authority of incoming call, by **checking** whether the time period during which incoming access request is received, is valid. Before processing the incoming access request, a change-root command is executed. The proxy agent initiates a connection to network **component** on behalf of source of access request.

ADVANTAGE - Provides **firewall** system that is resistant to conventional modes of attacks by hackers. Provides standalone fire-wall system that physically resides between point of public access and network **component** to be protected. **Verifies** authority of incoming request, without unduly burdening system resources. Avoids service attacks, without need to shutdown the port.

Dwg.4A,4B/
4

Title Terms: FIRE; WALL; SYSTEM; PROTECT; NETWORK; **COMPONENT** ; ROUTER; SERVE; DATABASE; HOST; MODEM; AGENT; **VERIFICATION** ; **AUTHORISE** ; INCOMING; CALL; **CHECK** ; TIME; PERIOD; INCOMING; ACCESS; REQUEST; RECEIVE ; VALID

Derwent Class: T01

International Patent Class (Main): G06F-012/14

File Segment: EPI

8/5/17

DIALOG(R)File 350:Derwent WPIX

011844932 **Image available**

WPI Acc No: 1998-261842/199823

XRPX Acc No: N98-206389

Firewall **for controlling access between two computer systems - uses** tunnelling **mechanism to operate on both sides of wall to set up outside-in connections when requested by trusted** objects **or users outside wall**

Patent Assignee: INT BUSINESS MACHINES CORP (IBMC); IBM UK LTD (IBMC)

Inventor: JADE P; MOORE V S; RAO A M; WALTERS G R

Number of Countries: 029 Number of Patents: 011

Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
WO 9818248	A1	19980430	WO 97GB2712	A	19971002	199823	B
EP 932965	A1	19990804	EP 97943996	A	19971002	199935	
			WO 97GB2712	A	19971002		
BR 9705094	A	19990629	BR 975094	A	19971020	199937	
CZ 9901387	A3	19990811	WO 97GB2712	A	19971002	199937	
			CZ 991387	A	19971002		
US 5944823	A	19990831	US 96731800	A	19961021	199942	
BR 9712635	A	19991026	BR 9712635	A	19971002	200009	
			WO 97GB2712	A	19971002		
TW 362177	A	19990621	TW 97107568	A	19970603	200028	
US 6061797	A	20000509	US 96731800	A	19961021	200030	
			US 98132915	A	19980812		
JP 2000505270	W	20000425	WO 97GB2712	A	19971002	200031	
			JP 98519056	A	19971002		
HU 200000336	A2	20000628	WO 97GB2712	A	19971002	200039	
			HU 2000336	A	19971002		
KR 2000048930	A	20000725	WO 97GB2712	A	19971002	200116	
			KR 99702966	A	19990406		

Priority Applications (No Type Date): US 96731800 A 19961021; US 98132915 A 19980812

Cited Patents: No-SR.Pub

Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
WO 9818248	A1	E	18	H04L-029/06	

Designated States (National): BR CA CN CZ HU JP KR PL RU
Designated States (Regional): AT BE CH DE DK ES FI FR GB GR IE IT LU MC NL PT SE

EP 932965	A1 E		H04L-029/06	Based on patent WO 9818248
Designated States (Regional): AT BE CH DE ES FR GB IE IT LI NL SE				
BR 9705094	A		H04L-029/06	
CZ 9901387	A3		H04L-029/06	Based on patent WO 9818248
US 5944823	A		G06F-011/00	
BR 9712635	A		H04L-029/06	Based on patent WO 9818248
TW 362177	A		G06F-013/10	
US 6061797	A		G06F-012/14	Cont of application US 96731800 Cont of patent US 5944823
JP 2000505270	W	26	H04L-012/66	Based on patent WO 9818248
HU 200000336	A2		H04L-029/06	Based on patent WO 9818248
KR 2000048930	A		H04L-029/06	Based on patent WO 9818248

Abstract (Basic): WO 9818248 A

The **tunnelling** apparatus for a **data** communication network including a fire-wall (1) which defines outside and inside regions and forms a security barrier. This prevents **objects** in the outside region from accessing **objects** in the inside region, while **objects** in the inside region are **permitted** to access **objects** in the outside region. An outside interface computer (3) is located in the outside region, and an inside interface computer (2) interfaces between the **firewall** and **objects** in the inside region.

A device in both the computers is provided for determining the identities of predetermined trusted **objects** in the inside region to which access is allowed from the outside region. A device in the outside computer responds to a request sent from an **object** in the outside region and cooperates with the determining device to **check** if the request is directed to one of the trusted **objects** . If the request is so directed the request is routed to the inside interface computer. A device in both interface computers responds to the request directed to the trusted **object** for forming a data communication connection to the outside **object** . The segments of the data connection located in the inside region and extending through the **firewall** are formed under the exclusive control of the inside interface computer. A segment of the data communication connection extends from the outside interface computer to the **object** that sent the request and is formed under the control of the outside interface computer.

USE - For isolating computer an network resources inside **firewall** from networks, computers and computer applications outside wall.

ADVANTAGE - Provides for special ' **tunnelling** ' access from inside services to outside services.

Dwg.1/5

Title Terms: **FIREWALL** ; CONTROL; ACCESS; TWO; COMPUTER; SYSTEM; **TUNNEL** ; MECHANISM; OPERATE; SIDE; WALL; SET; UP; CONNECT; REQUEST; **OBJECT** ; USER ; WALL

Derwent Class: T01; W01

International Patent Class (Main): G06F-011/00; G06F-012/14; G06F-013/10; H04L-012/66; H04L-029/06

International Patent Class (Additional): G06F-013/00; G06F-013/16; H04L-009/32; H04L-012/28; H04L-012/46; H04L-012/56

File Segment: EPI

8/5/18

011407711 **Image available**

WPI Acc No: 1997-385618/199735

XRPX Acc No: N97-320996

Computer network communication method using encrypted network packets - having source computer requesting configuration from another computer that returns temporarily encrypted tunnel **records which can only be updated via** authorised **connection request**

Patent Assignee: RAPTOR SYSTEMS INC (RAPT-N)

Inventor: KRAEMER J A; LEVESQUE R H; NADKARNI A P
Number of Countries: 022 Number of Patents: 003
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
WO 9726735	A1	19970724	WO 97US667	A	19970116	199735	B
AU 9717487	A	19970811	AU 9717487	A	19970116	199747	
US 5825891	A	19981020	US 96586231	A	19960116	199849	
			US 97959919	A	19971029		

Priority Applications (No Type Date): US 96586231 A 19960116; US 97959919 A 19971029
Cited Patents: 4.Jnl.Ref; US 5099517; US 5161193; US 5235644; US 5442708; US 5444782
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
WO 9726735	A1	E	26	H04L-009/00	
Designated States (National): AU CA IL JP					
Designated States (Regional): AT BE CH DE DK ES FI FR GB GR IE IT LU MC NL PT SE					
AU 9717487	A			H04L-009/00	Based on patent WO 9726735
US 5825891	A			H04L-009/00	Cont of application US 96586231

Abstract (Basic): WO 9726735 A

The method involves a communications system which has computers on different networks communicating over public network links. The transmissions include the use of encrypted messages and employ **firewall** computers (16,18) to interface the public (20) and internal (50,52) networks. To establish a communication path a source computer (54) sends a configuration request to a second computer.

The second computer creates a virtual **tunnel** record in its database and returns the **tunnel** record **information** to the source computer. This information is encrypted using a temporary encryption key. **Tunnel** records can be updated by connection requests that require the request to be **authorised** .

ADVANTAGE - Allows **firewall** computer to provide virtual **tunnel** records and secret keys and eliminate need for 'trusted computer'. Does not require user to generate **tunnel** records in order to communicate with **firewall** computer.

Dwg.2/11

Title Terms: COMPUTER; NETWORK; COMMUNICATE; METHOD; ENCRYPTION; NETWORK; PACKET; SOURCE; COMPUTER; REQUEST; CONFIGURATION; COMPUTER; RETURN; TEMPORARY; ENCRYPTION; **TUNNEL** ; RECORD; CAN; UPDATE; **AUTHORISE** ; CONNECT; REQUEST
Derwent Class: T01; W01
International Patent Class (Main): H04L-009/00
File Segment: EPI

11/5/1
DIALOG(R)File 350:Derwent WPIX

014123721 **Image available**
WPI Acc No: 2001-607931/200170
XRPX Acc No: N01-453880
System and method for controlling agent-authority connections via a firewall facilitates a tunnel action for a remote processor to contact a local processor via a reverse-authority device, a computer network and a firewall .
Patent Assignee: HEWLETT-PACKARD CO (HEWP)
Inventor: CLOUGH J; NELSON D S; SIT E N
Number of Countries: 002 Number of Patents: 002
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
DE 10052945	A1	20010830	DE 1052945	A	20001025	200170	B
JP 2001273211	A	20011005	JP 200137593	A	20010214	200173	

Priority Applications (No Type Date): US 2000504157 A 20000215
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
DE 10052945	A1		12	H04L-012/22	
JP 2001273211	A		11	G06F-013/00	

Abstract (Basic): DE 10052945 A1
NOVELTY - A group of supporting devices (110) links to a local processor (122) in a LAN (112). An authority engine (145) links a local computer (120) to the Internet (150). A remote computer (155) is also linked to the Internet. The local computer has a local processor (122), a computer memory and a client-device management gateway (CDMG) (125) to control the local processor.
USE - None given.
ADVANTAGE - The remote computer has a remote processor (157) and a supporting application (160) for communicating with the CDMG to control the supporting devices.
DESCRIPTION OF DRAWING(S) - The drawing shows a block diagram of a computer system specially adapted to run the present invention.
(Drawing includes non-English language text).
Group of supporting devices (110)
Local processor (122)
LAN (112)
Authority engine (145)
Local computer (120)
Internet (150)
Remote computer (155)
Local processor (122)
Client-device management gateway (125)
Remote processor (157)
Supporting application (160)
pp; 12 DwgNo 2/5
Title Terms: SYSTEM; METHOD; CONTROL; AGENT; **AUTHORISE** ; CONNECT; **FIREWALL** ; FACILITATE; **TUNNEL** ; ACTION; REMOTE; PROCESSOR; CONTACT; LOCAL; PROCESSOR; REVERSE; **AUTHORISE** ; DEVICE; COMPUTER; NETWORK; **FIREWALL**
Derwent Class: T01; W01
International Patent Class (Main): G06F-013/00; H04L-012/22
International Patent Class (Additional): H04L-012/24; H04L-012/56; H04L-012/58
File Segment: EPI

11/5/2
DIALOG(R)File 350:Derwent WPIX

014106894 **Image available**
WPI Acc No: 2001-591106/200167
XRPX Acc No: N01-440356

Secure access permitting **method for providing access between service external to network** firewall **and client internal to** firewall
Patent Assignee: HEWLETT-PACKARD CO (HEWP)
Inventor: HINDE S J; LOW C; WILCOCK L
Number of Countries: 025 Number of Patents: 001
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
EP 1081918	A2	20010307	EP 2000307357	A	20000825	200167	B

Priority Applications (No Type Date): GB 9920834 A 19990904
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
EP 1081918	A2	E	16	H04L-029/06	

Designated States (Regional): AL AT BE CH CY DE DK ES FI FR GB GR IE IT LI LT LU LV MC MK NL PT RO SE SI

Abstract (Basic): EP 1081918 A2

NOVELTY - The method involves **permitting** secure access between a service external to a network **firewall** , and a client internal to the **firewall** by establishing a ' **tunnel** ' through the **firewall** , carried by the HTTP messages. This opens communication **sockets** which the **Java Applet** and web server can use to communicate with each other.

DETAILED DESCRIPTION - The method for secure access between a service external to a network **firewall** and a client terminal internal to the **firewall** involves effecting an HTTP GET operation or equivalent from the client to establish a communications **socket** for communicating data from the service to the client. After a predetermined interval, another GET operation is effected to close the communications **socket** , irrespective of whether access between the service and the client is required to continue. The method is repeated while access between the service and the client is required to continue.

USE - Providing secure access through network **firewall** , between a service external to the network **firewall** e.g. a web page server, and a client internal to the **firewall** e.g. a web browser.

ADVANTAGE - Enables controlled secure connections using a versatile protocol e.g. TCP/IP to be established through a **firewall** and proxy server.

DESCRIPTION OF DRAWING(S) - The drawing shows a block diagram of a mechanism for communications from the server to the client.

pp; 16 DwgNo 5/5

Title Terms: SECURE; ACCESS; **PERMIT** ; METHOD; ACCESS; SERVICE; EXTERNAL; NETWORK; **FIREWALL** ; CLIENT; INTERNAL; **FIREWALL**
Derwent Class: T01; W01
International Patent Class (Main): H04L-029/06
File Segment: EPI

11/5/3
DIALOG(R)File 350:Derwent WPIX

014047494 **Image available**
WPI Acc No: 2001-531707/200159
XRPX Acc No: N01-394867
Secure web server for HTTP internet access to services requiring secure transfer of confidential data and user authentication
Patent Assignee: MONTIEL J (MONT-I)
Inventor: MONTIEL J
Number of Countries: 001 Number of Patents: 001
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
FR 2799077	A1	20010330	FR 9912260	A	19990927	200159	B

Priority Applications (No Type Date): FR 9912260 A 19990927
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
FR 2799077	A1		7	H04L-009/32	

Abstract (Basic): FR 2799077 A1

NOVELTY - The secure access control has a strong coupling between the web server and a **firewall** , using physical shielding and interconnection of hardware and software elements so that access to the server can be through the **firewall** only. A secure HTTP **tunnel** transports messages between the external client and the server. Messages are formatted in XML, and use strong encryption and **authentication** algorithms.

USE - Access to databases and e-commerce transactions

ADVANTAGE - Enhanced security in web-based database access and e-commerce transactions.

DESCRIPTION OF DRAWING(S) - The drawing shows a block schematic of the system (the drawing contains non-English language text).

pp; 7 DwgNo 2/3

Title Terms: SECURE; WEB; SERVE; ACCESS; SERVICE; REQUIRE; SECURE; TRANSFER ; CONFIDE; DATA; USER; AUTHENTICITY

Derwent Class: T01; W01

International Patent Class (Main): H04L-009/32

International Patent Class (Additional): G06F-017/60; H04L-012/28

File Segment: EPI

11/5/4

DIALOG(R)File 350:Derwent WPIX

013052597 **Image available**

WPI Acc No: 2000-224452/200019

XRPX Acc No: N00-168180

Security device for multi-level network system has two port RAM consisting two bus interfaces which are respectively connected to host bus and local bus

Patent Assignee: CRYPTEK SECURE COMMUNICATIONS LLC (CRYP-N)

Inventor: WILLIAMS T C

Number of Countries: 087 Number of Patents: 004

Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
WO 200010278	A2	20000224	WO 99US16416	A	19990721	200019	B
AU 200015954	A	20000306	AU 200015954	A	19990721	200030	
EP 1101161	A2	20010523	EP 99958627	A	19990721	200130	
			WO 99US16416	A	19990721		
US 6304973	B1	20011016	US 98129879	A	19980806	200164	

Priority Applications (No Type Date): US 98129879 A 19980806

Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
WO 200010278	A2	E	103	H04L-000/00	
	Designated States (National): AE AL AM AT AU AZ BA BB BG BR BY CA CH CN CU CZ DE DK EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MD MG MK MN MW MX NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT UA UG US UZ VN YU ZA ZW				
	Designated States (Regional): AT BE CH CY DE DK EA ES FI FR GB GH GM GR IE IT KE LS LU MC MW NL OA PT SD SE SL SZ UG ZW				
AU 200015954	A			H04L-000/00	Based on patent WO 200010278
EP 1101161	A2	E		G06F-003/00	Based on patent WO 200010278
	Designated States (Regional): AL AT BE CH CY DE DK ES FI FR GB GR IE IT LI LT LU LV MC MK NL PT RO SE SI				
US 6304973	B1			G06F-012/14	

Abstract (Basic): WO 200010278 A2

NOVELTY - A network interface connects the local bus of security device to network such as local area, Ethernet or ring network. A two port RAM has two bus interfaces, which are respectively connected to host bus and local bus such that the host computer and the client computer are connected.

DETAILED DESCRIPTION - An **authentication** interface is provided to **authenticate** the user. A CPU is provided for implementing firmware

and a cipher unit is connected to the local bus. An INDEPENDENT CLAIM is also included for data transmission and receiving control method.

USE - For multi-level network system.

ADVANTAGE - Prevents unauthorized access from host computer, since two-port RAM connects host bus and local bus using its two interface, thus security is improved. Reduces problems associated with traditional I and A device, intrusion detectors, **firewalls** and **VPNs** and previous MLS networks.

DESCRIPTION OF DRAWING(S) - The figure shows model diagram of secure network having security device.

pp; 103 DwgNo 1/14

Title Terms: SECURE; DEVICE; MULTI; LEVEL; NETWORK; SYSTEM; TWO; PORT; RAM; CONSIST; TWO; BUS; INTERFACE; RESPECTIVE; CONNECT; HOST; BUS; LOCAL; BUS

Derwent Class: T01; W01

International Patent Class (Main): G06F-003/00; G06F-012/14; H04L-000/00

International Patent Class (Additional): G06F-013/00

File Segment: EPI

11/5/5

DIALOG(R)File 350:Derwent WPIX

012679404 **Image available**

WPI Acc No: 1999-485511/199941

XRPX Acc No: N99-362540

Packet filter connected to private network provided with firewall **- has packet distributor which transmits data packets through private connection if packets contain** authenticating **data, otherwise, packets are transmitted from the** firewall **connection side**

Patent Assignee: HITACHI LTD (HITA)

Number of Countries: 001 Number of Patents: 001

Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
JP 11205388	A	19990730	JP 987682	A	19980119	199941	B

Priority Applications (No Type Date): JP 987682 A 19980119

Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
JP 11205388	A		13	H04L-012/66	

Abstract (Basic): JP 11205388 A

NOVELTY - A packet distributor (202) determines whether or not the data packet received through public connection contains **authenticating** information. If the packet contains such information, the distributor transmits the packet through private connection. Otherwise, the distributor transmits the packet from the fire wall connection side.

DETAILED DESCRIPTION - A packet forwarder (201) adds a predecided auhenticating information to the data packet received through a private connection and transmits the information to a public telecommunication network via a public connection. The forwarder also transmits data packets received from a **firewall** to the public communication network.INDEPENDENT CLAIMS are also include for the following:an **authenticating** server; a packet filtering procedure; a memory medium.

USE - For private network provided with **firewall** .

ADVANTAGE - Enables forwarding of real-time data by securing communication between private networks that comprise virtual private network **VPN** . Communication with other private networks can be executed through **firewall** . DESCRIPTION OF DRAWING(S) - The figure shows the internal block diagram of the packet filter. (201) Packet forwarder; (202) Packet distributor.

Dwg.2/14

Title Terms: PACKET; FILTER; CONNECT; PRIVATE; NETWORK; **FIREWALL** ; PACKET; DISTRIBUTE; TRANSMIT; DATA; PACKET; THROUGH; PRIVATE; CONNECT; PACKET; CONTAIN; AUTHENTICITY; DATA; PACKET; TRANSMIT; **FIREWALL** ; CONNECT; SIDE

Derwent Class: P85; W01

International Patent Class (Main): H04L-012/66

International Patent Class (Additional): G09C-001/00; H04L-009/32;

H04L-012/56
File Segment: EPI; EngPI

11/5/6
DIALOG(R)File 350:Derwent WPIX

012411205 **Image available**
WPI Acc No: 1999-217313/199919
XRPX Acc No: N99-160202
Firewall **packet** validation **for computer network**
Patent Assignee: LUCENT TECHNOLOGIES INC (LUCE)
Inventor: COSS M J; MAJETTE D L; SHARP R L
Number of Countries: 027 Number of Patents: 003
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
EP 909075	A1	19990414	EP 98307002	A	19980901	199919	B
JP 11168510	A	19990622	JP 98252830	A	19980907	199935	
US 6170012	B1	20010102	US 97928795	A	19970912	200103	

Priority Applications (No Type Date): US 97928795 A 19970912
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
EP 909075	A1	E	24	H04L-029/06	
	Designated States (Regional): AL AT BE CH CY DE DK ES FI FR GB GR IE IT LI LT LU LV MC MK NL PT RO SE SI				
JP 11168510	A		19	H04L-012/66	
US 6170012	B1			G06F-015/16	

Abstract (Basic): EP 909075 A1
NOVELTY - The method involves obtaining a session key for a packet of a given network session. A query portion of a rule is then processed. The query portion specifies a query to a cache containing information about packets which were previously processed by the **firewall** , when a match with the session key is not found in the cache, an action portion of the rule is processed as a function of a result of the query to the cache.
DETAILED DESCRIPTION - Cache look-up is performed and, if required, rule set look-up for the destination domain are carried out in a manner analogous to that employed for the source domain in step (504). During a step (508) if a rule that applies to the packet calls for an address change, e.g. to a proxy or for insertion of a tone packet into another (' **tunnel** option'), the process returns to step (505) for processing based on the changed destination.
USE - For preventing unauthorized access to computer networks using **firewall** protection.
ADVANTAGE - Improves processing efficiency; improves security; increases access rule flexibility, and enhances the ability of a **firewall** to deal with complex protocols. Computer network **firewall** is thus able to support multiple security policies and/or multiple users.
DESCRIPTION OF DRAWING(S) - The drawing as a partial flow chart of **firewall** processing for multiple domains.
pp; 24 DwgNo 5a/10
Title Terms: **FIREWALL** ; PACKET; VALID; COMPUTER; NETWORK
Derwent Class: P85; W01
International Patent Class (Main): G06F-015/16; H04L-012/66; H04L-029/06
International Patent Class (Additional): G06F-012/14; G06F-013/00; G06F-015/173; G09C-001/00; H04L-009/32; H04L-012/28; H04L-012/46
File Segment: EPI; EngPI

11/5/7
DIALOG(R)File 350:Derwent WPIX

012053068 **Image available**

WPI Acc No: 1998-469979/199841
XRPX Acc No: N98-366431
Packet switched network communications system for e.g. Internet - uses three proxies to establish end-to-end connection that navigate through the server firewalls **, with key communication occurring at middle proxy outside of user and client** firewalls
Patent Assignee: INT BUSINESS MACHINES CORP (IBMC); IBM CORP (IBMC)
Inventor: CRICHTON J M; GARVIN P F; STATEN J W; WRIGHT W L
Number of Countries: 004 Number of Patents: 005
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
GB 2323757	A	19980930	GB 983074	A	19980216	199841	B
JP 10285216	A	19981023	JP 9864914	A	19980316	199902	
KR 98079682	A	19981125	KR 983474	A	19980206	200004	
US 6104716	A	20000815	US 97828449	A	19970328	200041	
KR 261379	B1	20000701	KR 983474	A	19980206	200131	

Priority Applications (No Type Date): US 97828449 A 19970328
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
GB 2323757	A		29	H04L-029/06	
JP 10285216	A		19	H04L-012/56	
KR 98079682	A			H04L-012/56	
US 6104716	A			H04L-012/28	
KR 261379	B1			H04L-012/56	

Abstract (Basic): GB 2323757 A
The communications system using lightweight secure **tunnelling** protocol, comprises a users network with a server running a server application with a **firewall** [23] guarding the network [21]and including a software application enabling the **firewall** to make connections from inside to outside the **firewall** boundaries. To connect to a trusted client [222] the system utilises like facilities to establish a middle proxy [26] outside each **firewall** in an un-trusted network between the first and second network in communication.
The middle proxy is mutually addressable by both end proxies (using SOCKS on each **firewall**), a complete end-to-end connection between the client and their server [211] can be established. The connection is made using standard TCP/IP connection, with the end proxies [213,223] capable of connecting to a middle proxy anytime after it has been established. The two participants initiate security handshakes to provide a secure **tunnel** of communication.
ADVANTAGE - Allows an employee to **permit** an outside client to address his or her inside server. Bypasses controls put in place on the **firewall** .
Dwg.4/10
Title Terms: PACKET; SWITCH; NETWORK; COMMUNICATE; SYSTEM; THREE; ESTABLISH ; END; END; CONNECT; NAVIGATION; THROUGH; SERVE; **FIREWALL** ; KEY; COMMUNICATE; OCCUR; MIDDLE; USER; CLIENT; **FIREWALL**
Index Terms/Additional Words: **INTERNET** ,**SOCKS**, ; SOCKS,; LSTP
Derwent Class: T01; W01
International Patent Class (Main): H04L-012/28; H04L-012/56; H04L-029/06
International Patent Class (Additional): G06F-013/00
File Segment: EPI

11/5/9
DIALOG(R)File 350:Derwent WPIX

011407710 **Image available**
WPI Acc No: 1997-385617/199735
XRPX Acc No: N97-320995
Network packet handling method for sending encrypted packets over public network - receiving network packets at network interface computer and determining which virtual tunnel **each packet was sent over, before routing each packet to destination computer**

Patent Assignee: RAPTOR SYSTEMS INC (RAPT-N)
Inventor: KIRBY A J; KRAEMER J A; NADKARNI A P
Number of Countries: 022 Number of Patents: 003
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
WO 9726734	A1	19970724	WO 97US666	A	19970116	199735	B
AU 9718298	A	19970811	AU 9718298	A	19970116	199747	
US 5898784	A	19990427	US 96586230	A	19960116	199924	
			US 97963512	A	19971103		

Priority Applications (No Type Date): US 96586230 A 19960116; US 97963512 A 19971103
Cited Patents: US 5325362; US 5416842; US 5444782; US 5548646; US 5550984
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
WO 9726734	A1	E	30	H04L-009/00	
Designated States (National): AU CA IL JP					
Designated States (Regional): AT BE CH DE DK ES FI FR GB GR IE IT LU MC NL PT SE					
AU 9718298	A			H04L-009/00	Based on patent WO 9726734
US 5898784	A			H04L-009/00	Cont of application US 96586230

Abstract (Basic): WO 9726734 A

The method involves a communication system which has several computers connected to a number of internal networks linked by a public network, e.g. the Internet (RTM). The computers may communicate with one another at the application level using different protocols, e.g. TCP/IP,IPX. The computers can have drivers added such that their messages are encrypted prior to transmissions.

The networks can have **firewall** computers interfacing to the public network. The **firewall** computers use ''virtual **tunnels** '' to establish links between computers. The **firewalls** use the policy ID code to **identify** the destination computer and have databases to establish encryption and permissions.

ADVANTAGE - Has multiple **tunnels** between same two computers to allow packets that are encrypted with different algorithms to be sent between same computers. Spreads encryption load. Allows receiving computer to determine both packet's encryption algorithm and where packet should be routed.

Dwg.1/11

Title Terms: NETWORK; PACKET; HANDLE; METHOD; SEND; ENCRYPTION; PACKET; PUBLIC; NETWORK; RECEIVE; NETWORK; PACKET; NETWORK; INTERFACE; COMPUTER; DETERMINE; VIRTUAL; **TUNNEL** ; PACKET; SEND; ROUTE; PACKET; DESTINATION; COMPUTER
Derwent Class: T01; W01
International Patent Class (Main): H04L-009/00
File Segment: EPI

20/5/1
DIALOG(R)File 350:Derwent WPIX

014080630 **Image available**
WPI Acc No: 2001-564844/200163
Related WPI Acc No: 2001-343528; 2001-355373; 2001-610971
XRPX Acc No: N01-420519
Security architecture framework for netcentric computer system, comprises infrastructure for security services including core security components and tools
Patent Assignee: ANDERSEN CONSULTING LLP (ANDE-N)
Inventor: JONES R P; LUM R; SWAHN M
Number of Countries: 093 Number of Patents: 002
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
WO 200133359	A1	20010510	WO 2000US30420	A	20001103	200163	B
AU 200122489	A	20010514	AU 200122489	A	20001103	200163	

Priority Applications (No Type Date): US 99163477 P 19991103
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
WO 200133359	A1	E	57	G06F-011/30	

Designated States (National): AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CR CU CZ DE DK DM DZ EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT TZ UA UG UZ VN YU ZA ZW
Designated States (Regional): AT BE CH CY DE DK EA ES FI FR GB GH GM GR IE IT KE LS LU MC MW MZ NL OA PT SD SE SL SZ TR TZ UG ZW

AU 200122489	A		G06F-011/30	Based on patent WO 200133359

Abstract (Basic): WO 200133359 A1
NOVELTY - A computer security system comprises a security infrastructure and security services. The security infrastructure comprises core security components and security tools.
DETAILED DESCRIPTION - The security components of security infrastructure, include registration and identification, authentication single sign-on, access control, encryption, digital notarization, content and virus inspection, logging, non-repudiation, **firewall** , public key infrastructure, platform security and **virtual private networks** . INDEPENDENT CLAIMS are also included for the following:
(a) Method of operating netcentric security framework;
(b) Method for designing netcentric security framework;
(c) Method for designing and operating security framework
USE - For netcentric computer system used for business to consumer e-commerce and in complex network used in enterprise with remote offices, remote customers and users.
ADVANTAGE - The system protects the vital information, assets of an organization whether the organization is a business, non-profit or educational organization, a charity, a government office, or other useful enterprise, accesses the information at high speeds and also allows electronic transactions among computers and other corporate networks through internet.
DESCRIPTION OF DRAWING(S) - The figure shows the schematic diagram of the security architecture framework.
pp; 57 DwgNo 4/5
Title Terms: SECURE; ARCHITECTURE; FRAMEWORK; COMPUTER; SYSTEM; COMPRISE; SECURE; SERVICE; CORE; SECURE; COMPONENT; TOOL
Derwent Class: T01; W01
International Patent Class (Main): G06F-011/30
International Patent Class (Additional): H04L-009/00
File Segment: EPI

20/5/2
DIALOG(R)File 350:Derwent WPIX

014051246 **Image available**
WPI Acc No: 2001-535459/200159
Related WPI Acc No: 2000-490565
XRPX Acc No: N01-397581

Integrated telephony firewall **and scanner system for unauthorized access protection of private network, enables update of security policy based on VA result in accordance with result response policy**

Patent Assignee: SECURELOGIX CORP (SECU-N); BEEBE T (BEEB-I); COLLIER M D (COLL-I); CONYERS D (CONY-I); FAUSTINO S (FAUS-I); HAMLETT C (HAML-I)
Inventor: BEEBE T; COLLIER M D; CONYERS D; FAUSTINO S; HAMLETT C
Number of Countries: 002 Number of Patents: 002
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
US 20010014150	A1	20010816	US 98210347	A	19981211	200159	B
			US 99457494	A	19991208		
			US 2001761343	A	20010116		
AU 200119503	A	20010618	AU 200119503	A	20001206	200161	

Priority Applications (No Type Date): US 99457494 A 19991208; US 98210347 A 19981211; US 2001761343 A 20010116
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
US 20010014150	A1		44	H04M-003/00	CIP of application US 98210347 Cont of application US 99457494 Cont of patent US 6226372 CIP of patent US 6249575
AU 200119503	A			H04L-009/32	Based on patent WO 200143343

Abstract (Basic): US 20010014150 A1

NOVELTY - A call on an extension is detected together with the call attributes. Predetermines actions are performed based on the call attributes in accordance with a defined security rules. A vulnerability assessment (VA) is performed on the extension in response to a VA request. The security policy is updated based on the VA results in accordance with a result response policy.

DETAILED DESCRIPTION - A **firewall** and scanner client (28) defines the security policy with a security rule base, the result response policy and the extension groups. The security rule base comprises the security rules specifying actions to be taken based on the attributes of the call on the extension, while the result response policy comprises the result response rules specifying actions to be taken based on the VA results in the extension. The extension groups consists of number of extensions having at least one feature in common. An INDEPENDENT CLAIM is also included for an integrated telephony **firewall** and scanner system implementation method.

USE - For unauthorized access protection of private network or **virtual private network** of enterprise.

ADVANTAGE - Offers integrated telephony **firewall** and scanner system as standalone device or which can be applied over large-scale distributed client-server architecture. Ensures improved telecommunication **firewall** and scanner security capabilities, thereby ensuring implementation of corporate-dictated security structure and event visibility and report consolidation requirements. Enables automatic adjustment of security policy according to desire of enterprise personnel in response to security events. Enables proactive confirmation of security status of all modems and proactive identification of software or operating system controlling the modem.

DESCRIPTION OF DRAWING(S) - The figure shows the schematic block diagram of integrated telephony **firewall** and scanner system.

Firewall and scanner client (28)

pp; 44 DwgNo 1/12

Title Terms: INTEGRATE; TELEPHONE; **FIREWALL** ; SCAN; SYSTEM; ACCESS; PROTECT; PRIVATE; NETWORK; ENABLE; UPDATE; SECURE; BASED; RESULT; ACCORD; RESULT; RESPOND
Derwent Class: T01; W01
International Patent Class (Main): H04L-009/32; H04M-003/00
File Segment: EPI

20/5/3
DIALOG(R)File 350:Derwent WPIX

013156449 **Image available**
WPI Acc No: 2000-328321/200028
Related WPI Acc No: 1999-287395
XRPX Acc No: N00-247143
Communication link establishing method for computer network, involves receiving host name corresponding to requested address, responding to connection request and transmitting response back to terminal
Patent Assignee: NETWORK ENG SOFTWARE INC (NETW-N)
Inventor: COLEY C D; WESINGER R E
Number of Countries: 001 Number of Patents: 001
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
US 6052788	A	20000418	US 96733361	A	19961017	200028	B
			US 99299941	A	19990426		

Priority Applications (No Type Date): US 96733361 A 19961017; US 99299941 A 19990426
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
US 6052788	A		19	G06F-013/00	Cont of application US 96733361 Cont of patent US 5898830

Abstract (Basic): US 6052788 A
NOVELTY - The address of virtual host (116,118,166) is provided from DNS table on receiving DNS query from terminal and a connection request is transmitted. Host name corresponding to requested address is received from reverse DNS table. Address corresponding to name is obtained for use in subsequent network and connection is established. The response is transmitted in reverse direction to the terminal.
DETAILED DESCRIPTION - Forward and reverse DNS tables have entries of addresses of virtual hosts provided on **firewall** nodes corresponding to actual host. Virtual hosts are assigned to handle requests for actual host.
USE - For computer network.
ADVANTAGE - High level security is achieved as traffic cannot pass the **firewall** unless envoy is established. **Virtual private networks** can be established as two remote machines can communicate securely.
DESCRIPTION OF DRAWING(S) - The figure shows the block diagram of multilayered computer network.
Virtual host (116,118,166)
pp; 19 DwgNo 1/9
Title Terms: COMMUNICATE; LINK; ESTABLISH; METHOD; COMPUTER; NETWORK; RECEIVE; HOST; NAME; CORRESPOND; REQUEST; ADDRESS; RESPOND; CONNECT; REQUEST; TRANSMIT; RESPOND; BACK; TERMINAL
Derwent Class: T01
International Patent Class (Main): G06F-013/00
File Segment: EPI

20/5/4
DIALOG(R)File 350:Derwent WPIX

012902146 **Image available**
WPI Acc No: 2000-073982/200007
XRPX Acc No: N00-057929
Communication system using the internet
Patent Assignee: SUN MICROSYSTEMS INC (SUNM)
Inventor: PROVINO J E
Number of Countries: 004 Number of Patents: 005
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week

DE 19924575	A1	19991202	DE 1024575	A	19990528	200007	B
GB 2340702	A	20000223	GB 9912200	A	19990525	200013	
FR 2782873	A1	20000303	FR 996763	A	19990528	200019	
JP 2000049867	A	20000218	JP 99151071	A	19990531	200020	
GB 2340702	B	20000719	GB 9912200	A	19990525	200036	

Priority Applications (No Type Date): US 9887823 A 19980529
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
DE 19924575	A1		14	H04L-029/06	
GB 2340702	A			H04L-029/06	
FR 2782873	A1			H04L-012/56	
JP 2000049867	A		16	H04L-012/56	
GB 2340702	B			H04L-029/06	

Abstract (Basic): DE 19924575 A1

NOVELTY - The system provides a connection between a **virtual private network** (15) and external units via the internet (14). The connection between the external units is made using a service provider (11). The **virtual private network** has a **firewall** (30) and internal servers (31) for secondary addresses and name addresses.

USE - For use in network communication systems.

ADVANTAGE - Provides an improved system for communications using the internet.

DESCRIPTION OF DRAWING(S) - The drawing shows a schematic of the computer network.

Virtual network (15)

Internet (14)

Firewall (30)

Servers (31)

pp; 14 DwgNo 1/1

Title Terms: COMMUNICATE; SYSTEM
Derwent Class: T01; W01
International Patent Class (Main): H04L-012/56; H04L-029/06
International Patent Class (Additional): G06F-012/14; G06F-013/00; H04L-009/00; H04L-012/22; H04L-012/28; H04L-012/46
File Segment: EPI

20/5/5

DIALOG(R)File 350:Derwent WPIX
(c) 2002 Derwent Info Ltd. All rts. reserv.

012481287 **Image available**
WPI Acc No: 1999-287395/199927
Related WPI Acc No: 2000-328321
XRPX Acc No: N99-214644

Connection establishing method between remote computers

Patent Assignee: NETWORK ENG SOFTWARE (NETW-N)
Inventor: COLEY C D; WESINGER R E
Number of Countries: 001 Number of Patents: 001
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
US 5898830	A	19990427	US 96733361	A	19961017	199927	B

Priority Applications (No Type Date): US 96733361 A 19961017
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
US 5898830	A		22	G06F-001/00	

Abstract (Basic): US 5898830 A

NOVELTY - One bi-directional connection is established from first remote computer to one of the virtual hosts, and another bidirectional connection is established from one of the virtual hosts to second remote computer on behalf of first remote computer. The data is passed between the two remote computers using the two bi-directional connections.

DETAILED DESCRIPTION - An intermediate system is configured as

several virtual hosts each one responding to a network address used on one of the two computer networks. One of the virtual hosts is made to associate with an interface by mapping from the name of second remote computer to network address of one of the virtual hosts of intermediate system. A request for connection from first remote computer to second remote computer is received at interface by specifying name of second remote computer, and that request is routed to one of the virtual hosts according to mapping. INDEPENDENT CLAIMS are included for the following:

(a) **firewall** for selectively allowing connections between two remote computers;

(b) communication establishing method between two computers;

(c) computer readable medium

USE - For establishing connection between local and remote computers in multilayered computer enterprise network.

ADVANTAGE - Provides **firewall** that achieves maximum network security and maximum user convenience. Establishes **virtual private network** whereby two remote computers communicate securely, regardless of the degree of proximity of separation in the same manner as if the machines were on LAN.

DESCRIPTION OF DRAWING(S) - The figure shows block diagram of multilayered computer enterprise network.

pp; 22 DwgNo 1/9

Title Terms: CONNECT; ESTABLISH; METHOD; REMOTE; COMPUTER
Derwent Class: T01
International Patent Class (Main): G06F-001/00
File Segment: EPI

20/5/6

011407707 **Image available**
WPI Acc No: 1997-385614/199735
XRPX Acc No: N97-320992

Network linking network driver software security method - inserting security network driver between applications and real network drivers and selecting actions from libraries

Patent Assignee: RAPTOR SYSTEMS INC (RAPT-N)
Inventor: KIRBY A J; LEVESQUE R H
Number of Countries: 021 Number of Patents: 002
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
WO 9726731	A1	19970724	WO 97US640	A	19970116	199735	B
AU 9722426	A	19970811	AU 9722426	A	19970116	199747	

Priority Applications (No Type Date): US 96585765 A 19960116
Cited Patents: US 5086469; US 5416842
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
WO 9726731	A1	E	33	H04L-009/00	

Designated States (National): AU CA IL JP
Designated States (Regional): AT BE CH DE DK ES FI FR GB GR IE IT LU MC NL PT SE

AU 9722426	A		H04L-009/00	Based on patent WO 9726731

Abstract (Basic): WO 9726731 A

The communication system has computers on networks that can also be linked via public networks. Both secure transmission and **firewall** encapsulating are desired on transmissions. This is achieved by inserting a security network driver (72) between the applications (34) and the real external network driver (40). The driver encrypts and/or encapsulates the messages and either returns them to the application or to the network driver.

The security network driver has access to a number of libraries (76,90). These provide a selection of methods for encrypting and/or encapsulating the messages. The user may determine which methods are

used.

USE/ADVANTAGE - **Virtual private network** . Provides single point at which messages can be encrypted and firewalled allowing simply implemented progressive changes.

Dwg.3/11

Title Terms: NETWORK; LINK; NETWORK; DRIVE; SOFTWARE; SECURE; METHOD; INSERT; SECURE; NETWORK; DRIVE; APPLY; REAL; NETWORK; DRIVE; SELECT; ACTION

Derwent Class: T01; W01

International Patent Class (Main): H04L-009/00

File Segment: EPI

File 347:JAPIO OCT 1976-2001/Sep(UPDATED 020102)
(c) 2002 JPO & JAPIO

Set	Items	Description
S1	60	FIREWALL? ? OR (BASTION OR PROXY)()HOST? ? OR APPLICATION(-)(GATEWAY? ? OR GUARD? ?)
S2	18656	TUNNEL? OR VIRTUAL()PRIVATE()CONNECT? OR VPN OR VPNS
S3	367372	AUTHENTICAT? OR VERIF? OR VALIDAT? OR IDENTIF? OR SCREEN??? OR CHECK??? OR AUTHORIZ? OR AUTHORIS? OR PERMIT? OR PERMISSION
S4	17439	SOCKET? ? OR WINSOCK OR SSL
S5	1202033	OBJECT? ? OR CLASS?? OR INHERITANCE OR JAVA OR APPLET? ? OR COMPONENT? ?
S6	4921	(CONFIGUR? OR TUNNEL?)(3N)(DATA OR INFORMATION) OR PORT? ?(3N)(NUMBER? ? OR ADDRESS?? OR ID OR IDENTIF? OR IDENTIFICATION) OR SESSION? ?(3N)(ID OR IDENTIF? OR IDENTIFICATION OR DATA OR INFORMATION) OR (SECURITY OR TUNNEL?)(5N)CONFIGUR?
S7	1	S1 AND S6
S8	1	S7 OR (S7 AND S2:S5)
S9	2	S1 AND S2
S10	2	S9 OR (S9 AND S3:S6)
S11	43	S2 AND S4
S12	0	S1 AND S4
S13	3	S8 OR S10
S14	37	VIRTUAL()PRIVATE()NETWORK?
S15	0	S1 AND S14
S16	0	S4 AND S14
S17	0	AU="BROWNELL DAVID M" AND S1:S2

13/5/1
DIALOG(R)File 347:JAPIO
(c) 2002 JPO & JAPIO. All rts. reserv.

06464292 **Image available**
SYSTEM AND METHOD FOR FACILITATING COMMUNICATION BETWEEN DEVICE CONNECTED TO PUBLIC NETWORK SUCH AS INTERNET AND DEVICE CONNECTED TO NETWORK

PUB. NO.: 2000-049867 [JP 2000049867 A]
PUBLISHED: February 18, 2000 (20000218)
INVENTOR(s): PROVINO JOSEPH E
APPLICANT(s): SUN MICROSYST INC
APPL. NO.: 11-151071 [JP 99151071]
FILED: May 31, 1999 (19990531)
PRIORITY: 87823 [US 9887823], US (United States of America), May 29, 1998 (19980529)
INTL CLASS: H04L-012/56; G06F-013/00; H04L-012/46; H04L-012/28

ABSTRACT

PROBLEM TO BE SOLVED: To facilitate communication between devices respectively connected to a public network and a private network by transforming the human readable address by a name server connected through a secure **tunnel** to the private network to a network address.

SOLUTION: A device 12 (m) receives a message packet from a **firewall** 30. Concerning that packet, the encoded part is decoded by a secure packet processing function element 26, an integral Internet address related to the human readable Internet address is acquired, and that information is loaded to an IP parameter store 25. Afterwards, the device uses that integral internet address for generating a message packet for transmission to a server 31 (s) related to the human readable Internet address. Besides, when a name server 32 does not have such an integral Internet address, it is shown by a response message packet generated by the name server 32.

13/5/2
DIALOG(R)File 347:JAPIO
(c) 2002 JPO & JAPIO. All rts. reserv.

06263806 **Image available**
PACKET FILTER, **AUTHENTICATION** SERVER, PACKET FILTERING METHOD AND STORAGE MEDIUM

PUB. NO.: 11-205388 [JP 11205388 A]
PUBLISHED: July 30, 1999 (19990730)
INVENTOR(s): HASHIMOTO KAZUO
NISHIKADO TAKASHI
KAWAGUCHI KENJI
OTA MASATAKA
APPLICANT(s): HITACHI LTD
APPL. NO.: 10-007682 [JP 987682]
FILED: January 19, 1998 (19980119)
INTL CLASS: H04L-012/66; G09C-001/00; H04L-009/32; H04L-012/56

ABSTRACT

PROBLEM TO BE SOLVED: To provide the high speed packet filtering system that pre-vents a 3rd party from illegally intruding the internet **VPN** .

SOLUTION: The system is provided with a direct path connecting directly with a private network from the packet filter system 102, and a fire wall path via a **firewall** 106. The packet filter system 102 adds predetermined **authentication** information to a data packet received from a private network and sends the resulting packet to a public network and also sends the data packet received from the **firewall** 106 to the public network. The system 102 discriminates whether or not the data packet received from the public network is a data packet to which the **authentication** information

is added. When the data packet is a packet to which the **authentication** information is added, the **authentication** information is eliminated from the packet and the resulting data packet is sent to the private network. When the data packet is not a packet to which the **authentication** information is added, the resulting data packet is sent to the **firewall** 106.

13/5/3

06226948 **Image available**
PACKET **VERIFICATION** METHOD

PUB. NO.: 11-168510 [JP 11168510 A]
PUBLISHED: June 22, 1999 (19990622)
INVENTOR(s): COSS MICHAEL JOHN
MAJETTE DAVID L
SHARP RONALD L
APPLICANT(s): LUCENT TECHNOL INC
APPL. NO.: 10-252830 [JP 98252830]
FILED: September 07, 1998 (19980907)
PRIORITY: 928795 [US 928795], US (United States of America), September 12, 1997 (19970912)
INTL CLASS: H04L-012/66; G06F-013/00; G09C-001/00; H04L-009/32; H04L-012/46; H04L-012/28

ABSTRACT

PROBLEM TO BE SOLVED: To support a protocol (e.g. RealAudio(R) protocol) of a type that requires another additional network session returned to the user from an external device without the need of other application on a **firewall** .
SOLUTION: A computer network **firewall** **authenticates** or blocks a network session by using a dependence mask set based on **session** **data** items such as a .source host address, a destination host address and a service type. Using the dependence mask **identifies** number of **sessions** satisfying an inquiry made to a cache of the active session processed by the **firewall** . This inquiry corresponds to an access rule so that a session according to a specific rule is made dependent on the number adapted to the inquiry.

```
File 348:EUROPEAN PATENTS 1978-2002/Jan W04
         (c) 2002 European Patent Office
File 349:PCT FULLTEXT 1983-2002/UB=20020124,UT=20020117
         (c) 2002 WIPO/Univentio

Set     Items   Description
S1       2841   FIREWALL? ? OR (BASTION OR PROXY)()HOST? ? OR APPLICATION(-
            )(GATEWAY? ? OR GUARD? ?)
S2      23478   TUNNEL? OR VIRTUAL()PRIVATE()CONNECT? OR VPN OR VPNS
S3     613742   AUTHENTICAT? OR VERIF? OR VALIDAT? OR IDENTIF? OR SCREEN???
           OR CHECK??? OR AUTHORIZ? OR AUTHORIS? OR PERMIT? OR PERMISSI-
           ON
S4      36685   SOCKET? ? OR WINSOCK OR SSL
S5     825812   OBJECT? ? OR CLASS?? OR INHERITANCE OR JAVA OR APPLET? ? OR
           COMPONENT? ?
S6      30888   (CONFIGUR? OR TUNNEL?)(3N)(DATA OR INFORMATION) OR PORT? ?-
           (3N)(NUMBER? OR ADDRESS? OR ID OR IDENTIF???? OR IDENTIFICATI-
           ON) OR SESSION? ?(3N)(ID OR IDENTIF???? OR IDENTIFICATION OR -
           DATA OR INFORMATION) OR (SECURITY OR TUNNEL?)(5N)CONFIGUR?
S7        270   S1(S)S2
S8          6   S1(S)S2(S)S3(S)S4(S)S6
S9         31   S2(S)S4(S)S6
S10        54   S1(S)S2(S)S6
S11        38   S10 NOT S9
S12        30   S1(S)S3(S)S4(S)S6
S13        24   S12 NOT (S9 OR S11)
S14         0   S8 NOT S9:S13
S15      1148   VIRTUAL()PRIVATE()NETWORK?
S16        13   S15(S)S4(S)S6
S17         3   S16 NOT S8:S13
S18        25   S1(S)S15(S)S6
S19         3   S18 NOT (S8:S13 OR S17)
S20         0   AU="BROWNELL DAVID M" AND S1:S2
```

9/5,K/2 **(Item 2 from file: 348)**
DIALOG(R)File 348:EUROPEAN PATENTS

00919583
Pseudo network adapter for frame capture, encapsulation and encryption
Pseudonetzwerkadapter zur Rahmenaufnahme, -einkapselung und -verschlusselung
Adaptateur d'un pseudo-reseau pour la capture, l'encapsulation et le codage de trames

PATENT ASSIGNEE:
DIGITAL EQUIPMENT CORPORATION, (313085), 111 Powdermill Road, Maynard, Massachusetts 01754, (US), (applicant designated states: AT;BE;CH;DE;DK;ES;FI;FR;GB;GR;IE;IT;LI;LU;MC;NL;PT;SE)
INVENTOR:
Alden, Kenneth F., 188 Cross Street, Boylston, Massachusetts 01505, (US)
Lichtenberg, Mitchell P., 1339 Selo Drive, Sunnyvale, CA 94087, (US)
Wobber, Edward P., 460 Santa Monica Avenue, Menlo Park, California 94025, (US)
LEGAL REPRESENTATIVE:
Charig, Raymond Julian (79692), Eric Potter Clarkson, Park View House, 58 The Ropewalk, Nottingham NG1 5DD, (GB)
PATENT (CC, No, Kind, Date): EP 838930 A2 980429 (Basic)
APPLICATION (CC, No, Date): EP 97118556 971024;
PRIORITY (CC, No, Date): US 738155 961025
DESIGNATED STATES: AT; BE; CH; DE; DK; ES; FI; FR; GB; GR; IE; IT; LI; LU; MC; NL; PT; SE
INTERNATIONAL PATENT CLASS: H04L-029/06;

ABSTRACT EP 838930 A2
A new pseudo network adapter provides an interface for capturing packets from a local communications protocol stack for transmission on the virtual private network, and includes a Dynamic Host Configuration Protocol (DHCP) server emulator, and an Address Resolution Protocol (ARP) server emulator. The new system indicates to the local communications protocol stack that nodes on a remote private network are reachable through a gateway that is in turn reachable through the pseudo network adapter. A transmit path in the system processes data packets from the local communications protocol stack for transmission through the pseudo network adapter. An encryption engine encrypts the data packets and an encapsulation engine encapsulates the encrypted data packets into tunnel data frames. The network adapter further includes an interface into a transport layer of the local communications protocol stack for capturing received data packets from the remote server node, and a receive path for processing received data packets captured from the transport layer of the local communications protocol stack. The receive path includes a decapsulation engine, and a decryption engine, and passes the decrypted, decapsulated data packets back to the local communications protocol stack for delivery to a user.
ABSTRACT WORD COUNT: 194

LEGAL STATUS (Type, Pub Date, Kind, Text):
Assignee: 000531 A2 Transfer of rights to new applicant: Compaq Computer Corporation (687792) 20555 S.H. 249 Houston Texas. 77070 US
Application: 980429 A2 Published application (A1with Search Report ;A2without Search Report)
Change: 991013 A2 Legal representative(s) changed 19990825
LANGUAGE (Publication,Procedural,Application): English; English; English
FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS A	(English)	9818	1279
SPEC A	(English)	9818	11307
Total word count - document A			12586
Total word count - document B			0
Total word count - documents A + B			12586

...SPECIFICATION and encapsulates them into tunnel data frames.

The pseudo network adapter 382 then passes the **tunnel** **data** frames packets back to the TCP protocol layer 372 within the TCP/IP protocol stack through a conventional **socket** interface to the **tunnel** connection with the first node in the **tunnel** path.

The TCP protocol layer 372 then forms a TCP layer packet for each tunnel...

...464.

In the example embodiment of Fig. 19, the pseudo network adapter 459 passes the **data** to a **tunnel** application program 466. The **tunnel** application program 466 encrypts the IP packet received from the IP layer and encapsulates it into a **tunnel** **data** frame. The **tunnel** application then passes the **tunnel** **data** frame including the encrypted data to the **WinSock** interface 452, indicating a destination IP address of the remote **tunnel** end point. The **tunnel** **data** frame is then passed through the TCP layer 454, IP layer 456, NDIS MAC layer packet(s) received from the IP layer 478 and encapsulates them into **tunnel** **data** frames. The UNIX Daemon 486 then passes the **tunnel** **data** frames to the UNIX **socket** layer 474, through a **socket** associated with the **tunnel** connection. The **tunnel** **data** frames are then processed by the TCP layer 476, IP layer 478, data link layer...

9/5,K/3 (Item 1 from file: 349)

DIALOG(R)File 349:PCT FULLTEXT

00871315 **Image available**

SECURE AND RELIABLE DOCUMENT DELIVERY

LIVRAISON DE DOCUMENTS SURE ET FIABLE

Patent Applicant/Assignee:
PRIVATE EXPRESS TECHNOLOGIES PTE LTD, 21 Science Park Road, #02-01 The Aquarius, Singapore Science Park II, Singapore 117628, SG, SG (Residence), SG (Nationality)

Inventor(s):
ENG-WHATT Toh, Blk. 27, Balam Road, #16-31, Singapore 370027, SG,
CHEE-HONG Wong, Blk 103, Tao Ching Road, #09-02, Singapore 610103, SG,
KOK-HOON Teo, Blk. 83, Redhill Lane, #06-87, Singapore 150083, SG,
SEE-WAI Yip, Blk. 342, Choa Chu Kang Loop, #06-31, Singapore 680342, SG,

Legal Representative:
HENRY GOH (S) PTE LTD (agent), Toa Payoh Central, P.O. Box 183, Singapore 913107, SG,

Patent and Priority Information (Country, Number, Date):
Patent: WO 200205477 A2 20020117 (WO 0205477)
Application: WO 2001SG139 20010705 (PCT/WO SG0100139)
Priority Application: US 2000216734 20000707; US 2000242015 20001019; US 2000242014 20001019; US 2001887157 20010621

Designated States: AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CO CR CU CZ DE DK DM DZ EC EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT TZ UA UG UZ VN YU ZA ZW
(EP) AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE TR
(OA) BF BJ CF CG CI CM GA GN GW ML MR NE SN TD TG
(AP) GH GM KE LS MW MZ SD SL SZ TZ UG ZW
(EA) AM AZ BY KG KZ MD RU TJ TM

Main International Patent Class: H04L-009/00
Publication Language: English
Filing Language: English
Fulltext Availability:
Detailed Description
Claims
Fulltext Word Count: 15516

English Abstract
An Operations Center (OC) (200) acts as a central key manager and intermediary in securely, reliably and non-repudiably delivering a document (3) from a sender (100) to a recipient (300). The OC (200) acts as a key manager to facilitate the process of strong authentication of

the sender (100) and the recipient (300), encryption of the delivery (510), and setup of reliable connections (2A, 2B, 2C). In a preferred embodiment, the reliable connections (2A, 2B, 2C) are virtual private network connections.

French Abstract

L'invention concerne un centre des operations (OC) (200) qui agit comme gestionnaire central des cles et comme intermediaire dans une livraison sure, fiable et non repudiable d'un document (3) envoye par un expediteur (100) a un destinataire (300). Ce centre des operations (200) agit comme gestionnaire central des cles afin de faciliter le processus d'authentification forte de l'expediteur (100) et du destinataire (300), le codage de la livraison (510) et l'etablissement de connexions fiables (2A, 2B, 2C). Dans un mode de realisation prefere, ces connections fiables (2A, 2B, 2C) sont des connexions de reseau prive virtuel.

Legal Status (Type, Date, Text)

Publication 20020117 A2 Without international search report and to be republished upon receipt of that report.

Fulltext Availability:

Claims

Claim

... 3, the secure connection 2A is established 460 by use of a virtual private network (" **VPN** ") or an **SSL** connection. A **VPN** connection 2A could utilize protocols designed for layer 2 of the Open Systems Interconnection ("OSI") network architecture model, such as the Layer 2 **Tunneling** Protocol ("MP") or Point-to-Point **Tunneling** Protocol ("PPTP"). Alternately, the **VPN** connection 2A could be established using an OSI layer 3 protocol such as IP Security protocol ("IPSEC"). Alternatively, the **VPN** could be established at one of the layers in the host process subset (layers 5 through 7) of the OSI network architecture model. One benefit of establishing a **VPN** connection 2A at the host process subset layers is that present **VPN** systems employ protocols in layers 2 and 3. If the sender's computer system 100 is part of a network that already utilizes a **VPN** , a conflict may be created between the existing **VPN** and the **VPN** connection 2A attempting to be established 460 between the sending system I 00 and the OC 200. By creating a **VPN** connection 2A at the host process subset layers, the sender I 00 and the OC 200 can establish a **VPN** independent of any other **VPN** used by sender I 00's network. [00581 In one approach, the **VPN** connection 2A is created at the application level by using a session key and Hypertext...

...TCP"), or File Transfer Protocol ("FTP"). The secure connection modules 103 and 204 establish the **VPN** , by performing the following fimctions. Either the sending system's module 103 or the OC...

...session key. Once both parties have the session key, they
1 9
communicate via a **VPN** connection 2A that encrypts the application **data** with the **session** key. This process allows a compatible **VPN** **tunnel** to be created regardless of existing **VPN** setup in the sending system I 00, as described in commonly-assigned U.S. Provisional Patent Application No. 60/242,015, "Application **VPN** with Application Proxies," by Eng-Whatt Toh, filed 19 October 2000, which subject matter is incorporated herein by reference in its entirety. [00591 The **VPN** connection 2A has many advantages. One advantage is that data transmissions that occur over the **VPN** connection 2A carry additional encryption since they have been encrypted by the **VPN** encryption key (i.e., the session key). Second, the **VPN** 2A creates a reliable connection between the sender I 00 and OC 200. Traditional Internet...

...no one company or entity can guarantee reliable delivery or integrity of the message. The **VPN** 2A formed between the sending system I 00 and the OC 200 creates a pointit does not create an unnecessary audit trail. [00601 As a final example, the **VPN** -enabled OC 200 acts as central switch that can effectively extend the **VPN** connection 2A from the

sending system I 00 to the receiving system 300. Since a **VPN** connection is point-to-point, it is infeasible to produce a dynamic **VPN** connection that allows every possible sender I 00 to create a **VPN** to every possible recipient 3 00, without having a central key manager such as the ...

...sending an electronic document or receiving one, connects to the OC 200 by forming a **VPN** **tunnel** 2A,213. In this manner, a **VPN** connection 2A,213 is effectively created from the sending system I 00 to the receiving...

...with any recipient 300 using a secure and reliable delivery system. [00611 Once the secure **tunnel** 2A is formed between the sending system 100 and the OC 200, the sending system...system 300. As with the sending system 100, a secure connection 213, such as an **SSL** connection or a point-to-point **VPN** **tunnel** , is formed 550 between the OC 200 and receiving system 300. The receiving system 300...via a direct and secure connection 2C (FIG. 9), such as a peer-to-peer **VPN** connection or **SSL** connection. For example, the sending system 100 queries 525 the OC 200 to determine if...

...I 00 and the receiving system 300. Preferably, the secure connection 26
C is an **SSL** connection or a peer-to-peer **VPN** connection. Alternatively, the OC 200 could notify 614 the recipient 3 00 that the sender...

...via a direct and secure connection 2C (FIG. 9), such as a peer-to-peer **VPN** connection or **SSL** connection, when the receiving system 300 is not presently available to receive the delivery 510...

9/5,K/6 (Item 4 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT

00848841 **Image available**

METHOD AND SYSTEM FOR MANAGING AND CONFIGURING VIRTUAL PRIVATE NETWORKS
PROCEDE ET SYSTEME PERMETTANT DE GERER ET DE CONFIGURER DES RESEAUX VIRTUELS PRIVES

Patent Applicant/Assignee:
OPENREACH COM, Suite 104, 760 State Route 18, East Brunswick, NJ 08816-47907, US, US (Residence), US (Nationality), (For all designated states except: US)
Patent Applicant/Inventor:
KEANE John, 37 Memorial Parkway, Metuchen, NJ 08840-2138, US, US (Residence), US (Nationality), (Designated only for: US)
SHIMAMOTO Brion, 343 Riverside Avenue, Riversdie, CT 06878-2123, US, US (Residence), US (Nationality), (Designated only for: US)
HERRICK Michael, 20 Rimwood Lane, Colts Neck, NJ 07722-1348, US, US (Residence), US (Nationality), (Designated only for: US)
MACEY Christopher, 54 Elm Place, Red Bank, NJ 07701-1928, US, US (Residence), US (Nationality), (Designated only for: US)
HARWOOD Jonathan, 8 Post Road, Rumson, NJ 07760, US, US (Residence), US (Nationality), (Designated only for: US)
FRANCUS Jerold, 1017 Old Chester Road, Fair Hills, NJ 07931, US, US (Residence), US (Nationality), (Designated only for: US)
TUOMENOKSA Mark, 464 South Border Road, Winchester, MA 01890, US, US (Residence), US (Nationality), (Designated only for: US)
BENDINELLI Samuel, 36 Harvard Circle, Princeton, NJ 08540, US, US (Residence), US (Nationality), (Designated only for: US)
Legal Representative:
GARRETT Arthur S (et al) (agent), Finnegan, Henderson, Farabow, Garrett & Dunner, L .L.P., 1300 I Street, N.W., Washington, DC 20005-3315, US,

Patent and Priority Information (Country, Number, Date):
Patent: WO 200182533 A2 20011101 (WO 0182533)
Application: WO 2001US8970 20010322 (PCT/WO US0108970)
Priority Application: US 2000196297 20000412
Designated States: AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CO CR CU CZ DE DK DM DZ EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT TZ UA UG US UZ VN YU ZA ZW
(EP) AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE TR
(OA) BF BJ CF CG CI CM GA GN GW ML MR NE SN TD TG
(AP) GH GM KE LS MW MZ SD SL SZ TZ UG ZW
(EA) AM AZ BY KG KZ MD RU TJ TM
Main International Patent Class: H04L-012/46
Publication Language: English
Filing Language: English
Fulltext Availability:
Detailed Description
Claims
Fulltext Word Count: 26770

English Abstract
Methods and systems are provided for enabling a network between a first and a second processor using at least one additional processor separate from the first and second processors. In one embodiment, the at least one additional processor receives information indicating a consent on behalf of the first processor to enabling a tunnel between the first processor and the second processor and receives information indicating a consent on behalf of the second processor to enabling a tunnel between the second processor and the first processor. The at least one additional processor determines a first virtual address for the first processor and a second virtual address for the second processor such that the first and second virtual addresses uniquely identify the first and second processors, respectively, and are routable through the network. The at least one additional processor provides to each of the first and second processors the first and second virtual addresses to enable one or more tunnels between the first and the second processors.

French Abstract

Cette invention a trait a des procedes ainsi qu'a des systemes permettant d'activer un reseau entre un premier et un second processeurs au moyen d'au moins un processeur distinct des deux autres. Dans un mode de realisation, ce processeur supplementaire, celui-ci a tout le moins, recoit une information indiquant que le premier processeur accepte la mise en service d'un tunnel entre lui et le second processeur, de meme qu'il recoit une information indiquant que le second processeur accepte la mise en service d'un tunnel entre lui et le premier processeur. Ce processeur supplementaire, celui-ci a tout le moins, determine une premiere adresse virtuelle pour le premier processeur ainsi qu'une seconde adresse virtuelle pour le second processeur, de sorte que ces deux adresses virtuelles n'identifient, respectivement, que ces deux processeurs et qu'elles sont acheminables sur le reseau. Ce processeur supplementaire, celui-ci a tout le moins, fournit aux deux processeurs les deux adresses virtuelles afin de mettre en service entre eux un ou plusieurs tunnels.

Legal Status (Type, Date, Text)
Publication 20011101 A2 Without international search report and to be republished upon receipt of that report.
Correction 20011227 Corrections of entry in Section 1: under (71) replace "OPEANREACH. COM" by "OPENREACH. COM"
Republication 20011227 A2 Without international search report and to be republished upon receipt of that report.

Fulltext Availability:
Claims

Claim
... desires to configure as a gateway inciuding the computer serving as the computer 101. The **configured** gateway may then establish a
tunnel to another gateway (Le., similarly **configured** by the control system 175) after the control system 175 determines that each gateway mutually consents to enabling the **tunnel** and provides each gateway with sufficient **information** to enable the **tunnel** .
FIG. 3 shows an exemplary flowchart: for initially registering one or more gateways with the...

...Internet using a web browser to specify a particular configuration for a gateway. This specified **configuration information** may inciude a narne for the gateway and a name for the virtual private network...
...step 330). This disk image may include al(inverted exclamation mark) the program code and **information** needed to **configure** gateways 150-153 for establishing one or more virtual private networks established over communication channel...tunneis
between two or more gateways in the network 1 00; enabling the establishment of **tunnels** with gateways not accessible behind firewalls; and/or recovering the established virtual private networks after...

9/5,K/7 (Item 5 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT

00847466
METHODS AND SYSTEMS FOR PARTNERS IN VIRTUAL NETWORKS
PROCEDES ET SYSTEMES POUR ASSOCIES DANS DES RESEAUX VIRTUELS
Patent Applicant/Assignee:
OPENREACH COM, 760 State Route 18, Suite 104, East Brunswick, NJ 08816-4907, US, US (Residence), US (Nationality)
Inventor(s):
TUOMENOKSA Mark, 464 South Border Road, Winchester, MA 01890, US,
KEANE John, 37 Memorial Parkway, Metuchen, NJ 08840-2138, US,
LARSON Robert, 180 Hope Road, Tinton Falls, NJ 07724, US,
MACEY Christopher, 54 Elm Place, Red Bank, NJ 07701-1928, US,
Legal Representative:
GARRETT Arthur S (et al) (agent), Finnegan, Henderson, Farabow, Garrett & Dunner, L.L.P., 1300 I Street, N.W., Washington, DC 20005-3315, US,
Patent and Priority Information (Country, Number, Date):
Patent: WO 200180487 A2 20011025 (WO 0180487)
Application: WO 2001US11535 20010411 (PCT/WO US0111535)
Priority Application: US 2000196297 20000412; US 2001814178 20010322
Designated States: AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CO CR CU CZ DE DK DM DZ EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT TZ UA UG UZ VN YU ZA ZW
(EP) AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE TR
(OA) BF BJ CF CG CI CM GA GN GW ML MR NE SN TD TG
(AP) GH GM KE LS MW MZ SD SL SZ TZ UG ZW
(EA) AM AZ BY KG KZ MD RU TJ TM
Main International Patent Class: H04L-012/00
Publication Language: English
Filing Language: English
Fulltext Availability:
Detailed Description
Claims
Fulltext Word Count: 43500

English Abstract
Methods and systems are provided for enabling a network between a first and a second processor using at least one additional processor separate from the first and the second processors. In one embodiment, the additional processor may provide a set of names that includes the name of the second processor and receive on behalf of the first processor information indicating a selection that includes the name of the second processor. Further, the additional processor may provide a set of names that includes the name of the first processor and receives on behalf of the second processor information indicating a selection that includes the name of the first processor. The additional processor may determine a first virtual address for the first processor and a second virtual address for the second processor such that the first and second virtual addresses uniquely identify the first and second processors, respectively, and are routable through the network. The additional processor may provide to each of the first and second processors the first and second virtual addresses to enable one or more tunnels between the first and the second processors.

French Abstract
L'invention concerne des procedes et des systemes pour mettre en service un reseau entre un premier et un deuxieme processeur, au moyen d'au moins un processeur supplementaire separe des premier et deuxieme processeurs. Dans un mode de realisation, le processeur supplementaire peut fournir un ensemble de noms, comprenant le nom du deuxieme processeur et recevoir au nom du premier processeur des informations mentionnant une selection comportant le nom du deuxieme processeur. Par ailleurs, le processeur supplementaire peut fournir un ensemble de noms comprenant le nom du premier processeur et recevoir au nom du deuxieme processeur, des informations mentionnant une selection comprenant le nom du premier

processeur. Le processeur supplementaire peut determiner une premiere adresse virtuelle pour le premier processeur et une deuxieme adresse virtuelle pour le deuxieme processeur, de sorte que les premiere et deuxieme adresses virtuelles identifient individuellement les premier et deuxieme processeurs, et puissent etre acheminees sur le reseau. Le processeur supplementaire peut fournir a chacun des premier et deuxieme processeurs les premiere et deuxieme adresses virtuelles, pour la mise en service d'un ou plusieurs tunnels entre les premier et deuxieme processeurs.

Legal Status (Type, Date, Text)
Publication 20011025 A2 Without international search report and to be republished upon receipt of that report.
Examination 20020117 Request for preliminary examination prior to end of 19th month from priority date

Fulltext Availability:
Detailed Description

Detailed Description
... through a firewall. For example, when a user is prompted to select an allowable protocol, **port number** , and direction, the user may select a TCP **port number** at a gateway to serve as a destination port for al(inverted exclamation mark) TCP/IP packets received from the **tunnel** side of the firewall.

In another embodiment, a firewall maybe "on" anda(inverted exclamation mark...

9/5,K/8 (Item 6 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT

00846754 **Image available**
METHODS AND SYSTEMS FOR HAIRPINS IN VIRTUAL NETWORKS
PROCEDES ET SYSTEMES POUR CONTOURNEMENTS AUTORISES DANS DES RESEAUX VIRTUELS
Patent Applicant/Assignee:
OPENREACH COM, 760 State Route 18, Suite 104, East Brunswick, NJ 08816-4907, US, US (Residence), US (Nationality)
Inventor(s):
BENDINELLI Samuel, 36 Harvard Circle, Princeton, NJ 08540, US,
KEANE John, 37 Memorial Parkway, Metuchen, NJ 08840-2138, US,
MACEY Christopher, 54 Elm Place, Red Bank, NJ 07701-1928, US,
Legal Representative:
GARRETT Arthur S (et al) (agent), Finnegan, Henderson, Farabow, Garrett & Dunner, L.L.P., 1300 I Street, N.W., Washington, DC 20005-3315, US,
Patent and Priority Information (Country, Number, Date):
Patent: WO 200180522 A2 20011025 (WO 0180522)
Application: WO 2001US11541 20010411 (PCT/WO US0111541)
Priority Application: US 2000196297 20000412; US 2001814178 20010322
Designated States: AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CO CR CU CZ DE DK DM DZ EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT TZ UA UG UZ VN YU ZA ZW
(EP) AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE TR
(OA) BF BJ CF CG CI CM GA GN GW ML MR NE SN TD TG
(AP) GH GM KE LS MW MZ SD SL SZ TZ UG ZW
(EA) AM AZ BY KG KZ MD RU TJ TM
Main International Patent Class: H04L-029/06
Publication Language: English
Filing Language: English
Fulltext Availability:
Detailed Description
Claims
Fulltext Word Count: 43558

English Abstract
Methods and systems are provided for enabling communication between a first processor and a second processor using at least one additional processor separate from the first and second processors, wherein one or more firewalls selectively restrict the communication. In one embodiment, the additional processor may determine whether the first and second processors mutually consent to enabling a hairpin between the first and second processors. The first processor may be provided with a first informantion identifying the hairpin and the second processor may be provided with a second information identifying the hairpin, when the additional processor may determine that the first and second processors mutually consent to the hairpin. Moreover, a first information flow may be established from the first processor to the hairpin based on the provided first information, and a second information flow may be established from the second processor to the hairpin based on the provided second information. The hairpin may forward the first information flow received from the first processor to the second processor such that the communication between the first and second processors is allowed by the firewalls.

French Abstract
L'invention concerne des procedes et des systemes permettant une communication entre un premier processeur et un second processeur au moyen d'au moins un processeur supplementaire separe desdits premier et second processeurs, un ou plusieurs coupe-feu limitant selectivement la communication. Dans un mode de realisation, le processeur supplementaire peut determiner si lesdits premier et second processeurs admettent un contournement autorise de typehairpin entre eux. Le premier processeur peut detenir des premieres informations identifiant ce contournement autorise alors que le second processeur peut detenir des secondes informations identifiant ledit contournement, le processeur supplementaire pouvant alors etablir que lesdits premier et second processeurs admettent mutuellement ce contournement autorise. De plus, un premier flux d'informations peut etre etabli entre le premier processeur et le contournement autorise sur la base des premieres informations fournies, un second flux d'informations pouvant etre etabli entre le second processeur et le contournement autorise sur la base des secondes informations fournies. Ledit contournement peut transferer le premier flux d'informations recu entre le premier processeur et le second processeur de facon que la communication entre lesdits premier et second processeurs soit autorisee par les coupe-feu.

Legal Status (Type, Date, Text)
Publication 20011025 A2 Without international search report and to be republished upon receipt of that report.

Fulltext Availability:
Detailed Description

Detailed Description
... through a firewali. For example, when a user is prompted to select an allowable protocol, **port number** , and direction, the user may select a TCP **port number** at a gateway to serve as a destination port for afi TCP/IP packets received from the **tunnel** side of the firewall.

9/5,K/11 (Item 9 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT

00846727 **Image available**

METHODS AND SYSTEMS FOR ENABLING COMMUNICATION BETWEEN A PROCESSOR AND A NETWORK OPERATIONS CENTER

PROCEDES ET SYSTEMES PERMETTANT L'ETABLISSEMENT D'UNE COMMUNICATION ENTRE UN PROCESSEUR ET UN CENTRE D'EXPLOITATION DE RESEAU

Patent Applicant/Assignee:
OPENREACH COM, 760 State Route 18, East Brunswick, NJ 08816-4907, US, US (Residence), US (Nationality)
Inventor(s):
KEANE John, 37 Memorial Parkway, Metuchen, NJ 08840-2138, US,
BRUTMAN Neil R, 246 Mechanic Street, Red Bank, NJ 07701-2350, US,
HARRIS Michael J, 1351 White Oak Bottom Road, Toms River, NJ 08755-1336, US,
MACEY Christopher, 54 Elm Place, Red Bank, NJ 07701-1928, US,
Legal Representative:
GARRETT Arthur S (et al) (agent), Finnegan, Henderson, Farabow, Garrett & Dunner, L.L.P., 1300 I Street N.W., Washington, DC 20005-3315, US,

Patent and Priority Information (Country, Number, Date):
Patent: WO 200180489 A2 20011025 (WO 0180489)
Application: WO 2001US11537 20010411 (PCT/WO US0111537)
Priority Application: US 2000196297 20000412; US 2001814178 20010322
Designated States: AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CO CR CU CZ DE DK DM DZ EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT TZ UA UG UZ VN YU ZA ZW
(EP) AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE TR
(OA) BF BJ CF CG CI CM GA GN GW ML MR NE SN TD TG
(AP) GH GM KE LS MW MZ SD SL SZ TZ UG ZW
(EA) AM AZ BY KG KZ MD RU TJ TM
Main International Patent Class: H04L-012/00
Publication Language: English
Filing Language: English
Fulltext Availability:
Detailed Description
Claims
Fulltext Word Count: 33073

English Abstract
Methods and systems are provided for enabling a virtual network between a first processor and a second processor using at least one additional processor separate from the first and second processors. The additional processor may determine a first virtual address that identifies the first processor in the virtual network and provide the first virtual address to the first processor. When a tunnel between the first processor and the second processor is requested from the additional processor, the additional processor may authenticate the request based on the first virtual address and determine a second virtual address that identifies the second processor in the virtual network. After the additional processor authenticates the request and determines that the first and second processors have indicated a mutual consent for enabling one or more tunnels between the first and second processors, the additional processor may provide the second virtual address to the first processor to enable the requested tunnel between the first and second processors.

French Abstract
L'invention concerne des procedes et des systemes permettant d'etablir un reseau virtuel entre un premier processeur et un second processeur en utilisant au moins un processeur additionnel distinct du premier et du second processeur. Ce processeur additionnel peut definir une premiere adresse virtuelle identifiant le premier processeur dans le reseau virtuel et fournir cette premiere adresse virtuelle au premier processeur. Lorsque l'etablissement d'une tunnel entre le premier et le second processeur est demande au processeur additionnel, ce dernier peut authentifier cette demande au moyen la premiere adresse virtuelle et

definir une seconde adresse virtuelle qui identifie le second processeur dans le reseau virtuel. Apres que le second processeur a authentifie la demande et determine que le premier et le second processeur ont indique un consentement mutuel pour la mise en oeuvre d'un ou de plusieurs tunnels entre le premier et le second processeur, le processeur additionnel peut fournir la seconde adresse virtuelle au premier processeur afin de mettre en oeuvre le tunnel demande entre le premier et le second processeur.

Legal Status (Type, Date, Text)
Publication 20011025 A2 Without international search report and to be republished upon receipt of that report.
Examination 20020117 Request for preliminary examination prior to end of 19th month from priority date

Fulltext Availability:
Detailed Description

Detailed Description
... through a firewall. For example, when a user is prompted to select an allowable protocol, **port number** , and direction, the user may select a TCP **port number** at a gateway to serve as a destination port for al(inverted exclamation mark) TCP/IP packets received from the **tunnel** side of the firewali.

In another embodiment, a firewall maybe "on" and al(inverted exclamation ...

9/5,K/12 (Item 10 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT

00846726 **Image available**
METHODS AND SYSTEMS FOR MANAGING VIRTUAL ADDRESSES FOR VIRTUAL NETWORKS
PROCEDES ET SYSTEMES DE GESTION D'ADRESSES VIRTUELLES DANS DES RESEAUX VIRTUELS
Patent Applicant/Assignee:
OPENREACH COM, 760 State Route 18, East Brunswick, NJ 08816-4907, US, US (Residence), US (Nationality)
Inventor(s):
KEANE John, 37 Memorial Parkway, Metuchen, NJ 08840-2138, US,
MACEY Christopher, 54 Elm Place, Red Bank, NJ 07701-1928, US,
Legal Representative:
GARRETT Arthur S (et al) (agent), Finnegan, Henderson, Farabow, Garrett & Dunner, L.L.P., 1300 I Street, N.W., Washington, DC 20005-3315, US,
Patent and Priority Information (Country, Number, Date):
Patent: WO 200180488 A2 20011025 (WO 0180488)
Application: WO 2001US11536 20010411 (PCT/WO US0111536)
Priority Application: US 2000196297 20000412; US 2001814178 20010322
Designated States: AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CO CR CU CZ DE DK DM DZ EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT TZ UA UG UZ VN YU ZA ZW
(EP) AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE TR
(OA) BF BJ CF CG CI CM GA GN GW ML MR NE SN TD TG
(AP) GH GM KE LS MW MZ SD SL SZ TZ UG ZW
(EA) AM AZ BY KG KZ MD RU TJ TM
Main International Patent Class: H04L-012/00
Publication Language: English
Filing Language: English
Fulltext Availability:
Detailed Description
Claims
Fulltext Word Count: 43469

English Abstract
Methods and system are provided for enabling a virtual network between a

first processor and a second processor using at least one additional processor separate from the first processor and the second processor. In one embodiment, the at least one additional processor may determine a first virtual address and a first base address for the first processor such that the first virtual address is routable through the virtual network and the first base address is routable through a base network and determine a second virtual address and a second base address for the second processor such that the second virtual address is routable through the virtual network and the second base address is routable through the base network. The at least one additional processor may provide the first virtual address and the first base address to the first processor and the second virtual address and the second base address to the second processor. Moreover, the virtual network may be enabled over the base network based on the first virtual address, the first base address, the second virtual address, and the second base address.

French Abstract
L'invention concerne des procedes et des systemes permettant d'activer un reseau virtuel entre un premier processeur et un second processeur au moyen d'au moins un processeur additionnel, separe du premier et du second processeur. Dans un mode de realisation, le processeur additionnel peut determiner une premiere adresse virtuelle et une premiere adresse de base pour le premier processeur, de facon que la premiere adresse virtuelle puisse etre acheminee par le reseau virtuel et que la premiere adresse de base puisse etre acheminee par un reseau de base. Ce processeur peut en outre determiner une seconde adresse virtuelle et une seconde adresse de base pour le second processeur, de facon que la seconde adresse virtuelle puisse etre acheminee par le reseau virtuel et que la seconde adresse de base puisse etre acheminee par le reseau de base. Le processeur additionnel peut fournir la premiere adresse virtuelle et la premiere adresse de base au premier processeur et la seconde adresse virtuelle et la seconde adresse de base au second processeur. Le reseau virtuel, par ailleurs, peut etre active sur le reseau de base, sur la base de la premiere adresse virtuelle, de la premiere adresse de base, de la seconde adresse virtuelle et de la seconde adresse de base.

Legal Status (Type, Date, Text)
Publication 20011025 A2 Without international search report and to be republished upon receipt of that report.

Fulltext Availability:
Detailed Description

Detailed Description
... through a firewall. For example, when a user is prompted to select an allowable protocol, **port number** , and direction, the user may select a TCP **port number** at a gateway to serve as a destination port for al(inverted exclamation mark) TCP/IP packets received from the **tunnel** side of the firewall.

In another embodiment, a firewall maybe "on" and all client side...

9/5,K/13 (Item 11 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT

00846345 **Image available**
METHODS AND SYSTEMS FOR USING NAMES IN VIRTUAL NETWORKS
PROCEDE ET SYSTEMES POUR UTILISER DES NOMS DANS DES RESEAUX VIRTUELS
Patent Applicant/Assignee:
OPENREACH COM, 760 State Route 18, East Brunswick, NJ 08816-4907, US, US (Residence), US (Nationality)
Inventor(s):
TUOMENOKSA Mark, 464 South Border Road, Winchester, MA 01890, US,
Legal Representative:
GARRETT Arthur S (et al) (agent), Finnegan, Henderson, Farabow, Garrett &

Dunner, L.L.P., 1300 I Street, N.W., Washington, DC 20005-3315, US,
Patent and Priority Information (Country, Number, Date):
Patent: WO 200180037 A2 20011025 (WO 0180037)
Application: WO 2001US11540 20010411 (PCT/WO US0111540)
Priority Application: US 2000196297 20000412; US 2001814178 20010322
Designated States: AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CO CR CU
CZ DE DK DM DZ EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR
KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ PL PT RO RU SD SE
SG SI SK SL TJ TM TR TT TZ UA UG UZ VN YU ZA ZW
(EP) AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE TR
(OA) BF BJ CF CG CI CM GA GN GW ML MR NE SN TD TG
(AP) GH GM KE LS MW MZ SD SL SZ TZ UG ZW
(EA) AM AZ BY KG KZ MD RU TJ TM
Main International Patent Class: G06F-015/163
Publication Language: English
Filing Language: English
Fulltext Availability:
Detailed Description
Claims
Fulltext Word Count: 43655

English Abstract
Methods and systems are provided for enabling a network between a first and a second processor using at least on additional processor separate from the first and the second processors. In one embodiment, the additional processor may receive on behalf of the first processor information that includes the name of the second processor and receives on behalf of the second processor information that includes the name of the first processor. The additional processor may determine a first virtual address for the first processor based on the received name of the first procesor and a seocnd virtual address for the second processor based on the received name of the second processor such that the first and second virtual addresses uniquely identify the first and second processors, respectively, and are routable through the network. The additional processor may provide to each of the first and second processors the first and second virtual addresses to enable one or more tunnels between the first and the second processors.

French Abstract
L'invention concerne des procedes et des systemes, permettant d'etablir un reseau entre une premiere et une seconde unite de traitement et consistant a utiliser au moins une unite de traitement supplementaire separee des premiere et seconde unites de traitement. Selon une realisation, l'unite de traitement supplementaire peut recevoir, pour le compte de la premiere unite de traitement, des informations relatives au nom de la seconde unite de traitement et recevoir, pour le compte de la seconde unite de traitement, des informations relatives au nom de la premiere unite de traitement. Ladite unite de traitement supplementaire peut determiner une premiere adresse virtuelle pour la premiere unite de traitement, a partir du nom de la premiere unite de traitement recu, et une seconde adresse virtuelle pour la seconde unite de traitement, a partir du nom de la seconde unite de traitement recu, de sorte que les premiere et seconde adresses virtuelles identifient univoquement les premiere et seconde unites de traitement, respectivement, et puissent etre acheminees a travers ledit reseau. L'unite de traitement supplementaire peut delivrer aux premiere et seconde unites de traitement les premiere et seconde adresses virtuelles respectives, pour etablir au moins un tunnel entre les premiere et seconde unites de traitement.

Legal Status (Type, Date, Text)
Publication 20011025 A2 Without international search report and to be republished upon receipt of that report.

Fulltext Availability:
Detailed Description

Detailed Description
... through a firewall. For example, when a user is prompted to select an

allowable protocol, **port number** , and direction, the user may select a TCP **port number** at a gateway to serve as a destination port for al(inverted exclamation mark) TCP/IP packets received from the **tunnel** side of the firewall.

In another embodiment, a firewall maybe "on" and al(inverted exclamation ...

9/5,K/14 (Item 12 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT

00845284
METHODS AND SYSTEMS FOR TRANSACTIONAL TUNNELING
PROCEDES ET SYSTEMES DE TRANSMISSION TUNNEL DE TRANSACTIONS
Patent Applicant/Assignee:
BLUESTREAK COM, 76 Hammarlund Way, Middletown, RI 02842, US, US (Residence), US (Nationality), (For all designated states except: US)
Patent Applicant/Inventor:
CROY John Charles, 21 Bailey Avenue, Middletown, RI 02842, US, US (Residence), US (Nationality), (Designated only for: US)
Legal Representative:
DAMMAN Kirk A (et al) (agent), Foley, Hoag & Eliot LLP, One Post Office Square, Boston, MA 02109, US,
Patent and Priority Information (Country, Number, Date):
Patent: WO 200177968 A2 20011018 (WO 0177968)
Application: WO 2001US11692 20010410 (PCT/WO US0111692)
Priority Application: US 2000195933 20000410
Parent Application/Grant:
Related by Continuation to: US 2000195933 20000410 (CIP)
Designated States: AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CO CR CU CZ DE DK DM DZ EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT TZ UA UG US UZ VN YU ZA ZW
(EP) AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE TR
(OA) BF BJ CF CG CI CM GA GN GW ML MR NE SN TD TG
(AP) GH GM KE LS MW MZ SD SL SZ TZ UG ZW
(EA) AM AZ BY KG KZ MD RU TJ TM
Main International Patent Class: G06F-017/60
Publication Language: English
Filing Language: English
Fulltext Availability:
Detailed Description
Claims
Fulltext Word Count: 6510

English Abstract

French Abstract
L'invention concerne des procedes et des systemes qui permettent d'executer une transaction electronique, comprenant l'analyse des pages d'un serveur web qui execute une transaction afin de separer le contenu statique du contenu transactionnel, l'identification et le stockage de regles d'execution de transaction sur le site, et la presentation d'affichages permettant a l'utilisateur d'achever la transaction sans interagir directement avec le site, p. ex. en interagissant avec une banderole publicitaire, un courrier electronique, un telephone cellulaire ou une autre interface simple.

Legal Status (Type, Date, Text)
Publication 20011018 A2 With declaration under Article 17(2)(a); without abstract; title not checked by the International Searching Authority.
Correction 20011220 Corrected version of Pamphlet front pages: under (57) delete abstract
Republication 20011220 A2 With declaration under Article 17(2)(a); without

abstract; title not checked by the International Searching Authority.

Fulltext Availability:
Detailed Description

Detailed Description
... data from one server to another in a computer network. Referring to Fig. 1, conventional **tunneling** involves moving **data** from one virtual private network (**VPN**) or host I 1 0 to another host 1 12 using a protocol, such as the Pointto-Point protocol of Microsoft Corporation. **Tunneling** typically uses encryption to encode data, such as RC4 encryption from RSA, which is a fast stream cipher, or Secure **Socket** 3o Layer (**SSL**) encryption, which is a widely available public key cryptography scheme distributed by Netscape Corporation. **SSL** is supported in almost all browsers and web server technologies. **Tunneling** also implies that once a connection 114 is established between servers, it remains open over...

9/5,K/15 (Item 13 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT

00844673 **Image available**
SYSTEM AND METHOD FOR PROJECTING CONTENT BEYOND FIREWALLS
SYSTEME ET PROCEDE PERMETTANT DE PROJETER DES CONTENUS AU-DELA DE COUPE-FEU
Patent Applicant/Assignee:
SCIENCE APPLICATIONS INTERNATIONAL CORPORATION, 10260 Campus Point Drive, MS #F3, San Diego, CA 92121-1578, US, US (Residence), US (Nationality), (For all designated states except: US)
Patent Applicant/Inventor:
STEPHENSON Mark M, 5435 South Dayton-Brandt Rd., New Carlisle, OH 45344, US, US (Residence), US (Nationality), (Designated only for: US)
WALTERS Steven A, 474 Lookout Ridge, Dayton, OH 45419, US, US (Residence), US (Nationality), (Designated only for: US)
Legal Representative:
GLEMBOCKI Christopher R (et al) (agent), Banner & Witcoff, Ltd., 1001 G Street, N.W., Eleventh Floor, Washington, DC 20001-4597, US,
Patent and Priority Information (Country, Number, Date):
Patent: WO 200178349 A2 20011018 (WO 0178349)
Application: WO 2001US11706 20010411 (PCT/WO US0111706)
Priority Application: US 2000196096 20000411; US 2001824132 20010403
Parent Application/Grant:
Related by Continuation to: US 2000196096 20000411 (CON); US 2001824132 20010403 (CON)
Designated States: AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CO CR CU CZ DE DK DM DZ EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT TZ UA UG US UZ VN YU ZA ZW
(EP) AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE TR
(OA) BF BJ CF CG CI CM GA GN GW ML MR NE SN TD TG
(AP) GH GM KE LS MW MZ SD SL SZ TZ UG ZW
(EA) AM AZ BY KG KZ MD RU TJ TM
Main International Patent Class: H04L-029/00
Publication Language: English
Filing Language: English
Fulltext Availability:
Detailed Description
Claims
Fulltext Word Count: 15973

English Abstract
A system and method for exchanging information between clients separated by firewalls is disclosed. A server may receive the information as posted through a browser client from beyond a first firewall and relay it to another client beyond a second firewall without lowering the security levels of the firewalls.

French Abstract
La presente invention concerne un systeme et un procede permettant d'echanger des informations entre des clients qui sont separes par des coupe-feu. Un serveur peut recevoir les informations telles que postees par un client d'explorateur a partir d'au-dela d'un premier coupe-feu et les transmet a un autre client se trouvant au-dela d'un second coupe-feu, sans abaisser les niveaux de securite desdits coupe-feu.

Legal Status (Type, Date, Text)
Publication 20011018 A2 Without international search report and to be republished upon receipt of that report.
Examination 20020110 Request for preliminary examination prior to end of 19th month from priority date

Fulltext Availability:
Detailed Description

Detailed Description
... users and system managers to securely enter infori-nation such as usernarnes, passwords, and server **configuration data** . Other secure network networking techniques such as **VPN** may be employed or, in less critical application, standard unencrypted protocols may be used.

1581...

9/5,K/17 (Item 15 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT

00830336 **Image available**
METHOD OF CALL CONTROL TO MINIMIZE DELAYS IN LAUNCHING MULTIMEDIA OR VOICE CALLS IN A PACKET-SWITCHED RADIO TELECOMMUNICATIONS NETWORK
PROCEDE DE REGULATION DES APPELS PERMETTANT DE REDUIRE LES DELAIS A UN MINIMUM LORS DE L'ETABLISSEMENT D'APPELS MULTIMEDIA OU VOCAUX DANS UN RESEAU DE TELECOMMUNICATIONS A COMMUTATION DE PAQUETS
Legal Representative:
MAGNUSSON Monica (agent), Ericsson Radio Systems AB, Patent Unit Radio Access, S-164 80 Stockholm, SE,
Patent and Priority Information (Country, Number, Date):
Patent: WO 200163947 A1 20010830 (WO 0163947)
Application: WO 2001SE219 20010206 (PCT/WO SE0100219)
Priority Application: US 2000510964 20000221
Designated States: AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CR CU CZ DE DK DM DZ EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT TZ UA UG UZ VN YU ZA ZW
(EP) AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE TR
(OA) BF BJ CF CG CI CM GA GN GW ML MR NE SN TD TG
(AP) GH GM KE LS MW MZ SD SL SZ TZ UG ZW
(EA) AM AZ BY KG KZ MD RU TJ TM
Main International Patent Class: H04Q-007/22
International Patent Class: H04Q-007/38
Publication Language: English
Filing Language: English
Fulltext Availability:
Detailed Description
Claims
Fulltext Word Count: 4867

English Abstract
A method of call control in a packet-switched radio telecommunication network that minimizes delays in launching a voice call from a first Internet Protocol (IP)-based mobile station (MS(11)) to a second IP-based MS (12). The method includes the steps of preventing voice traffic from being routed to an Internet Service Provider (ISP), and setting up an optimized path for voice traffic from the first MS to the second MS. The

optimized path may be set up by creating (48, 49, 63, 64, 65) a shortest route tunnel (53) between a first serving GPRS service node (SGSN1(13)) serving the first MS and a second SGSN (SGSN2(14)) serving the second MS. Alternatively, the tunnel (66) may be established (48, 49, 63, 64, 65) between the base station controllers (BSCs(61, 62)) of each MS's serving radio base station.

French Abstract
Procede de regulation des appels dans un reseau de telecommunications radio a commutation de paquets, qui permet de reduire a un minimum les delais lors de l'etablissement d'un appel vocal d'une premiere station mobile (MS (11)) basee sur un protocole Internet (IP) vers une seconde MS (12) basee sur un IP. Ledit procede consiste a empecher le trafic de voix d'etre achemine vers un fournisseur de services Internet (ISP) et a etablir un chemin optimise pour le trafic de voix de la premiere MS a la seconde MS. Le chemin optimise peut etre etabli par creation (48, 49, 63, 64, 65) d'un tunnel (53) d'itineraire le plus court entre un premier noeud de service GPRS (SGSN1(13)) desservant la premiere MS et un second SGSN (SGSN2(14)) desservant la seconde MS. Alternativement, le tunnel (66) peut etre etabli (48, 49, 63, 64, 65) entre les dispositifs de commande (BSCs(61, 62)) de chaque station de base radio desservant les stations mobiles.

Legal Status (Type, Date, Text)
Publication 20010830 A1 With international search report.
Publication 20010830 A1 Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.
Examination 20011206 Request for preliminary examination prior to end of 19th month from priority date

Fulltext Availability:
Detailed Description

Detailed Description
... At a minimum, the information elements include the IMSIs of the two MSs, the media **port numbers** , and the **address** I 0 of SGSN2. When the new GTP message is received by SGSNI, SGSNI verifies...

...and a PDP context, and then creates a new GTP message called the Real Time **Tunnel** Build Request message 51 containing the media channel numbers, IMSIs, and PDP context. The Real Time **Tunnel** Build Request message is then sent to SGSN2. SGSN2 verifies that the MM context and...

...PDP context related 1 5 to MS2 exist, and if so, sends a Real Time **Tunnel** Build Request Acknowledgment message 52 back to SGSNL
A bidirectional **tunnel** is then created at 53 between SGSNI and SGSN2 for
the direct routing of any payload from the RTP media **sockets** for MS I and MS2. The anchor SGSNI sends a GTP Create Optimal **Tunnel** Acknowledgment message 54 to GGSN I confirming that the **tunnel** is now created. GGSNI then sends an Open InterSGSN Turuiel Acknowledgment message 55 to CSCF1 confin-ning the optimized **tunnel** . CSCF1 informs CSCF2 of the creation of the **tunnel** at 56 which, in turn, informs GGSN2 at 57 and SGSN2 at 58.

11/5,K/5 (Item 1 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT

00864375
SYSTEM AND METHOD FOR SECURE MANAGEMENT OF REMOTE SYSTEMS
SYSTEME ET PROCEDE DE GESTION SECURISEE DE DISPOSITIFS A DISTANCE
Patent Applicant/Assignee:
NETWOLVES CORPORATION, Suite 740, 2502 Rocky Point Drive, Tampa, FL 33607 , US, US (Residence), US (Nationality)
Inventor(s):
STEPHENS Daniel Guy Jr, 1845 Nebraska Avenue, NE, St. Petersburg, FL 33702, US,
POWALI Edwin, 16217 Sawgrass Circle, Tampa, FL 33624, US,
LOMBARD Stephen, 6912 14th Street North, St. Petersburg, FL 33702, US,
Legal Representative:
KUESTER Jeffrey R (agent), Thomas, Kayden, Horstemeyer & Risley, LLP, Suite 1750, 100 Galleria Parkway, NW, Atlanta, GA 30339-5948, US,
Patent and Priority Information (Country, Number, Date):
Patent: WO 200197019 A2 20011220 (WO 0197019)
Application: WO 2001US18934 20010613 (PCT/WO US0118934)
Priority Application: US 2000211399 20000614; US 2000702483 20001031
Designated States: AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CO CR CU CZ DE DK DM DZ EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT TZ UA UG UZ VN YU ZA ZW
(EP) AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE TR
(OA) BF BJ CF CG CI CM GA GN GW ML MR NE SN TD TG
(AP) GH GM KE LS MW MZ SD SL SZ TZ UG ZW
(EA) AM AZ BY KG KZ MD RU TJ TM
Main International Patent Class: G06F-009/00
Publication Language: English
Filing Language: English
Fulltext Availability:
Detailed Description
Claims
Fulltext Word Count: 10877

English Abstract
A secure system and method for managing and monitoring remote devices preferably includes periodic pulling of configuration information from an accessible platform rather than pushing information from a central site. In one implementation, an electronic mail system is used as a staging platform in combination with a defined polling arrangement to transfer encrypted configuration information in a robust and secure method for updating remote device configurations.
French Abstract
Procede et systeme securises servant a gerer et a controler des dispositifs a distance, ce qui consiste, de preference, a extraire periodiquement des informations de configuration depuis une plate-forme accessible, plutot qu'a pousser des informations depuis un site central. Dans un mode de realisation, on utilise un systeme de courrier electronique en tant que plate-forme de simulation combinee a un systeme defini d'appels selectifs afin de transferer des informations de configuration chiffrees au moyen d'un procede robuste et securise de mise a jour de configurations de dispositifs a distance.

Legal Status (Type, Date, Text)
Publication 20011220 A2 Without international search report and to be republished upon receipt of that report.

Fulltext Availability:
Detailed Description

Detailed Description
... WO 01/97019 PCT/USO1/18934
9
data 301 for the gateway server. The example **configuration data** 301

shows a file (or other data structure in other embodiments) having **configuration information** regarding administration and gateway fimetions. The importance of this configuration infonnation will become apparent below during the discussion of the installation of portions of the **configuration data** 301 onto the gateway servers (FIG. 7C, later discussed). The administration machine 2 1 0 (FIG. 2) may reconfigure host information, device setup, **firewall** filters and definitions, email settings, and other parameters of the gateway servers. For example, the ...

...web cache; Squid web cache; Samba file sharing; DNS and bind; (inverted exclamation mark)pfilter **firewall** rules; ipnat (inverted exclamation mark)p address redirection; ipeonfig set (inverted exclamation mark)p address and hostnames; route manage routes; web access control; add users, groups, mail; **VPN** ip **tunneling** , intrusion detection sub-system. Another grouping of such infonnation in one implementation includes.

5 ip...

11/5,K/6 (Item 2 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT

00842527 **Image available**
ARCHITECTURE AND PACKET ROUTING IN A MULTI-BEARER-TYPE NETWORK
ARCHITECTURE ET ACHEMINEMENT DE PAQUETS DANS UN RESEAU DE TYPE MULTISUPPORT
Patent Applicant/Assignee:
NOKIA OYJ, Keilalahdentie 4, FIN-02150 Espoo, FI, FI (Residence), FI (Nationality), (For all designated states except: US)
Patent Applicant/Inventor:
XU Lin, Vilppulanpolku 4 A 1, FIN-33720 Tampere, FI, FI (Residence), CN (Nationality), (Designated only for: US)
PAILA Toni, Everstinkuja 1 C 66, FIN-02600 Espoo, FI, FI (Residence), FI (Nationality), (Designated only for: US)
Legal Representative:
KOLSTER OY AB (agent), Iso Roobertinkatu 23, P.O. Box 148, FIN-00121 Helsinki, FI,
Patent and Priority Information (Country, Number, Date):
Patent: WO 200176286 A1 20011011 (WO 0176286)
Application: WO 2001FI306 20010329 (PCT/WO FI0100306)
Priority Application: FI 2000752 20000331
Designated States: AE AG AL AM AT AT (utility model) AU AZ BA BB BG BR BY BZ CA CH CN CO CR CU CZ CZ (utility model) DE DE (utility model) DK DK (utility model) DM DZ EE EE (utility model) ES FI FI (utility model) GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ PL PT RO RU SD SE SG SI SK SK (utility model) SL TJ TM TR TT TZ UA UG US UZ VN YU ZA ZW
(EP) AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE TR
(OA) BF BJ CF CG CI CM GA GN GW ML MR NE SN TD TG
(AP) GH GM KE LS MW MZ SD SL SZ TZ UG ZW
(EA) AM AZ BY KG KZ MD RU TJ TM
Main International Patent Class: H04Q-007/22
International Patent Class: H04Q-007/38
Publication Language: English
Filing Language: English
Fulltext Availability:
Detailed Description
Claims
Fulltext Word Count: 7150

English Abstract
A method for routing data packets (DP) to a mobile node (MN) from its correspondent node (CN), via a multi-bearer network, or MBN. The MBN comprises uplink bearer networks (GSM, GPRS, UMTS) and downlink bearer networks (DxB). The method comprises: 1) storing an address (202) associated with a centralized traffic policy controller (TPC) as the

mobile node's care-of address in its home agent (HA); 2) routing an initial data packet via the home agent and the centralized traffic policy controller to a bearer network interface unit (DxB IU, DL IU) serving the mobile node; 3) storing an address (214) of the bearer network interface unit as the mobile node's care-of address in the correspondent node (CN); 4) routing subsequent data packets from the correspondent node (CN) to the bearer network interface unit (DxB IU, DL IU), whereby the home agent (HA) and the centralized traffic policy controller are bypassed.

French Abstract
L'invention porte sur un procede d'acheminement de paquets de donnees (DP) d'un noeud mobile (MN) a son noeud correspondant (CN), via un reseau multisupport ou MBN. Le MBN comprend des reseaux supports a liaison montante (GSM, GPRS, UMTS) et des reseaux supports a liaison descendante (DxB). Le procede consiste a: 1) stocker une adresse (202) associee a un controleur centralise de politique de trafic (TPC) comme une adresse de prise en pension du noeud mobile au niveau de son agent domicile (HA); 2) acheminer un paquet initial de donnees via l'agent domicile et le controleur centralise de politique de trafic vers une unite d'interface de reseau support (DxB<u> </u>IU, DL<u> </u>IU) desservant le noeud mobile; 3) stocker une adresse (214) de l'unite d'interface du reseau support comme adresse de prise en pension du noeud mobile dans le noeud correspondant (CN); 4) acheminer les paquets de donnees suivants du noeud correspondant (CN) vers l'unite d'interface du reseau support (DxB<u> </u>IU, DL<u> </u>IU), ce qui fait qu'on court-circuite l'agent domicile (HA) et le controleur centralise de politique de trafic.

Legal Status (Type, Date, Text)
Publication 20011011 A1 With international search report.
Examination 20011227 Request for preliminary examination prior to end of 19th month from priority date

Fulltext Availability:
Claims

Claim
... The home agent is a routing entity in a mobile node's home network which **tunnels** packets for delivery to the mobile node when it is away from its home network...QoS indication is a case where a (Transmission Control Protocol) data packet header indicates a **port number** which in turn indicates the QoS requirement. It should be understood that'quality of service...

...border gateway BG is typically a simple (but sufficiently powerful) router which preferably includes a **firewall** function FW. A backbone network BB combines the different bearer networks BN. The backbone network...The home agent is a routing entity in a mobile node's home network which **tunnels** packets for delivery to the mobile node when it is away from its home network, and maintains current location information for the mobile node. It **tunnels** datagrams for delivery to, and detunnels datagrams from, a mobile node when the mobile node...

...may route the first data packet(s) of new sessions but does not route subsequent **data** packets of ongoing **sessions** if the MN sends its updated mobility binding information to the CN. The traffic control...

...time, only one COA is registered as the primary COA to which the home agent **tunnels** MN-terminated **data** .
The home agent HA knows the care-of address associated with the traffic controller TPC...

...and route the data to its final destination even if the HA encrypts MN-terminated **tunnelled data** .
According to a preferred feature of the invention, the primary COA registered in the home...The MN and the CN may open a second session in parallel to the first **session** . The **data** packets of the parallel session may be routed directly to the MN via the IU...

...data from any CN. When the first packet arrives from a CN, the packet is **tunnelled** by the HA to the MN's COA associated with the TPC. The TPC, acting...first user data packet is routed to the HA. (In Figure 7, 'data' refers to **data** packets of **session** 1, and ' **data** 2' refers to **data** packets of **session** 2.) In step SS6, because the HA stores the TPC's IP address as the MN's primary COA, the packet is **tunnelled** to the TPC. In step SS8, the TPC uses the QMTC table to classify the...the MN, and the new session requires best effort service (no resource reservation needed), the **data** of the new **session** is sent just like the data in step SS32 (the final step being shown by...

11/5,K/8 (Item 4 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT

00817128 **Image available**
METHOD AND SYSTEM FOR COMMUNICATION
PROCEDE ET SYSTEME DE COMMUNICATION
Legal Representative:
BERGENTALL Annika (et al) (agent), Cegumark AB, P.O. Box 53047, S-400 14 Goteborg, SE,
Patent and Priority Information (Country, Number, Date):
Patent: WO 200150688 A1 20010712 (WO 0150688)
Application: WO 2000SE2565 20001218 (PCT/WO SE0002565)
Priority Application: SE 994841 19991229
Designated States: AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CR CU CZ DE DK DM DZ EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT TZ UA UG UZ VN YU ZA ZW
(EP) AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE TR
(OA) BF BJ CF CG CI CM GA GN GW ML MR NE SN TD TG
(AP) GH GM KE LS MW MZ SD SL SZ TZ UG ZW
(EA) AM AZ BY KG KZ MD RU TJ TM
Main International Patent Class: H04L-012/46
International Patent Class: H04L-012/56; H04L-009/00
Publication Language: English
Filing Language: English
Fulltext Availability:
Detailed Description
Claims
Fulltext Word Count: 9325

English Abstract
A method and a system for establishing a connection between a first computer of a first computer network and a resource of a second computer network via a third network through a gateway intervening between the second computer network and the third network. A requester issues a request for a connection from the first computer to the resource by specifying a name of the resource. A temporary IP number is returned to the first computer in answer to the request. The temporary IP number is mapped to a tunnel to the gateway. The gateway administrates the handling of data packets such that data packets addressed by the first computer to the temporary IP number, arriving through the tunnel, are routed to the resource and data packets arriving from the resource destined to the first computer, are routed through the tunnel to the first computer.

French Abstract
L'invention concerne un procede et un systeme permettant d'etablir une liaison entre un premier ordinateur d'un premier reseau informatique et une ressource d'un deuxieme reseau informatique via un troisieme reseau par une passerelle intervenant entre le deuxieme reseau informatique et le troisieme reseau. Un demandeur emet une demande de liaison entre le premier ordinateur et la ressource en specifiant un nom de ressource. Un numero IP temporaire est renvoye au premier ordinateur en reponse a la demande. Le numero IP temporaire est mis en correspondance avec un tunnel vers la passerelle. La passerelle administre la gestion des paquets de donnees de telle facon que les paquets de donnees adresses par le premier

ordinateur au numero IP temporaire, arrivant par le tunnel, sont achemines jusqu'a la ressource et les paquets de donnes arrivant de la ressource et destines au premier ordinateur, sont achemines par le tunnel jusqu'au premier ordinateur.

Legal Status (Type, Date, Text)
Publication 20010712 A1 With international search report.
Examination 20011004 Request for preliminary examination prior to end of 19th month from priority date

Fulltext Availability:
Detailed Description
Detailed Description
... it, and thus have the possibilities of the invention. The inten-nediate system 230 will **configure** at least one **tunnel** 231 from the intennediate system to the **firewall** /gateway 226 of the second domain 220. A **tunnel** is a logical network connection between two processes, encapsulating the traffic during transport. Traffic over such a connection is 1 5 traditionally encrypted to prevent eavesdropping. The **tunnel** or **tunnels** are preferably authenticated at regular, or irregular, intervals.

'fhe intermediate system 230 will intercept DNS...local IP number ? 583 yes from 582: get mapping/table to find out where, which **tunnel** , to route the **data** package,
5 584 from 583: translate (remap) the source IP number, the IP number of ...

...IP number of the first computer according to the table (map),
586 from 585: transfer **data** packet in appropriate **tunnel** according to table
(map)
587 no from 5 8 1: other processing,
588 no from...

11/5,K/9 (Item 5 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT

00814176
A SCHEME FOR DETERMINING TRANSPORT LEVEL INFORMATION IN THE PRESENCE OF IP SECURITY ENCRYPTION
SCHEMA POUR DETERMINER L'INFORMATION SUR LE NIVEAU DE TRANSPORT EN PRESENCE DE CRYPTAGE DE SECURITE IP
Patent Applicant/Assignee:
NOKIA CORPORATION, Keilalahdentie 4, FIN-02150 Espoo, FI, FI (Residence), FI (Nationality)
Patent Applicant/Inventor:
KOODLI Rajeev, 5 Kansas Street #5, Natick, MA 01760, US, US (Residence), IN (Nationality)
SENGODAN Senthil, 3 Albert Drive #3, Woburn, MA 01801, US, US (Residence), IN (Nationality)
Legal Representative:
STOUT Donald E (et al) (agent), Antonelli, Terry, Stout and Kraus, LLP, Suite 1800, 1300 North Seventeenth Street, Arlington, VA 22209, US,
Patent and Priority Information (Country, Number, Date):
Patent: WO 200147169 A2 20010628 (WO 0147169)
Application: WO 2000US34991 20001226 (PCT/WO US0034991)
Priority Application: US 99471083 19991223
Designated States: AE AG AL AM AT AU AZ BA BB BG BR BY CA CH CN CR CU CZ DE DK DM DZ EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT TZ UA UG UZ VN YU ZA ZW
(EP) AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE TR
(OA) BF BJ CF CG CI CM GA GN GW ML MR NE SN TD TG
(AP) GH GM KE LS MW MZ SD SL SZ TZ UG ZW

(EA) AM AZ BY KG KZ MD RU TJ TM
Main International Patent Class: H04L
Publication Language: English
Filing Language: English
Fulltext Availability:
Detailed Description
Claims
Fulltext Word Count: 7082

English Abstract
A method and apparatus which permits access, by intermediate nodes between source and destination nodes, to selected information such as transport level information, normally included in a payload of a packet upon which encrypting security processing has been performed according to an encrypting security protocol. In the present invention, prior to performing encrypting security processing on the packet, according to the security protocol, information related to selected information normally included in a payload of the packet is stored in a field in the header of the packet where the field is not subject to the encrypting security processing. Thereafter, encrypting security processing according to the security protocol is performed on the packet. The packet including the header having stored therein information corresponding to the selected information normally included in the payload and the payload upon which encrypting security processing has been performed is then transmitted on the packet switched network to its destination. Since the information related to the selected information normally included in the payload of the packet is stored in the header of the packet, access to the selected information by the intermediate nodes between source and destination nodes in a packet switched network is possible.

French Abstract
L'invention concerne un procede et un dispositif permettant d'acceder, par des noeuds intermediaires entre des noeuds d'origine et des noeuds de destination, a une information selectionnee, telle que l'information sur le niveau de transport, comprise en temps normal dans la capacite utile d'un paquet ayant fait l'objet d'un traitement de securite par cryptage, selon un protocole de securite par cryptage. Selon l'invention, avant d'effectuer le traitement de securite par cryptage, selon le protocole de securite, il est prevu de stocker l'information concernant l'information selectionnee qui se trouve de maniere generale dans la capacite utile du paquet, dans une zone situee dans l'en-tete du paquet, ou la zone n'est pas soumise au traitement de securite par cryptage. Le paquet est ensuite soumis au traitement de securite par cryptage, selon le protocole de securite. Le paquet comprenant l'en-tete dans lequel est stockee l'information correspondant a l'information selectionnee se trouvant de maniere generale incluse dans la charge utile, ainsi que la charge utile ayant ete soumise au traitement de securite par cryptage sont ensuite transmis sur le reseau de commutation de paquets, a destination. L'information concernant l'information selectionnee comprise de maniere generale dans la charge utile du paquet etant stockee dans l'en-tete du paquet, l'acces a l'information selectionnee par les noeuds intermediaires entre les noeuds d'origine et les noeuds de destination dans un reseau de commutation de paquets est possible.

Legal Status (Type, Date, Text)
Publication 20010628 A2 Without international search report and to be republished upon receipt of that report.
Examination 20011108 Request for preliminary examination prior to end of 19th month from priority date
Fulltext Availability:
Detailed Description

Detailed Description
... level information of importance here are 5 the transport protocol (TCP/UDP/ICMP) and the **port number** . The mechanism was discussed for transport mode, **tunnel** mode and nested ESP protocol security processings. Using such mechanisms, inten-nediate nodes such as diff-serv markers/classifiers, **firewalls** /policers as well as network management

nodes can perform their respective functions. These nodes require...

11/5,K/17 (Item 13 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT

00766059 **Image available**
QUERY INTERFACE TO POLICY SERVER
INTERFACE D'INTERROGATION VERS SERVEUR DE REGLES
Patent Applicant/Inventor:
HANNEL Clifford Lee, 3178 Futura Point, Thousand Oaks, CA 91362, US, US (Residence), US (Nationality), (Designated only for: US)
MAY Anthony Allan, 6644 Glade Avenue #217, Woodland Hills, CA 91303, US, US (Residence), CA (Nationality), (Designated only for: US)
Legal Representative:
NELSON Gordon E, 57 Central Street, P.O. Box 782, Rowley, MA 01969, US
Patent and Priority Information (Country, Number, Date):
Patent: WO 200079434 A1 20001228 (WO 0079434)
Application: WO 2000US17078 20000621 (PCT/WO US0017078)
Priority Application: US 99140417 19990622
Designated States: AU JP SG US
(EP) AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE
Main International Patent Class: G06F-017/30
Publication Language: English
Filing Language: English
Fulltext Availability:
Detailed Description
Claims
Fulltext Word Count: 54190

English Abstract
A scalable access filter that is used together with others like it in a virtual private network to control access by users at clients in the network to information resources provided by servers in the network. Each access filter use a local copy of an access control data base (3845) to determine whether an access request is made by a user. Each user belongs to one or more user groups and each information ressource belongs to one or more information sets. Access is permitted or denied according to access policies which define access in terms of the user groups and information sets. The first access filter in the path performs the access check, encrypts and authenticates the request; the other access filters in the path do not repeat the access check. The interface used by applications to determine whether a user has access to an entity is now an SQL query. The policy server (3811) assembles the information needed for the response to the query from various information sources, including source external to the policy server.

French Abstract
L'invention concerne un filtre d'acces scalaire utilise avec d'autres filtres similaires dans un reseau prive virtuel afin de controler l'acces des utilisateurs a des clients du reseau pour obtenir des ressources d'informations fournies par des serveurs sur le reseau. Chaque filtre d'acces utilise une copie locale d'une base de donnees de controle d'acces (3845) pour determiner si la demande d'acces est effectuee par un utilisateur. Chaque utilisateur appartient a au moins un groupe d'utilisateurs et chaque ressource d'informations appartient a au moins un ensemble d'informations. L'acces est autorise ou refuse en fonction des politiques d'acces qui definissent l'acces en terme des groupes d'utilisateurs et des ensembles d'informations. Le premier filtre d'acces dans la voie effectue la verification d'acces, decrypte, et authentifie la demande, les autres filtres d'acces dans la voie ne repetent pas la verification d'acces. L'interface utilisee par les applications pour determiner si un utilisateur a acces a une entite est alors une demande SQL. Le serveur de regles (3811) assemble les informations requises pour la reponse a la demande emanant de plusieurs sources d'informations, y compris une source externe audit serveur.

Legal Status (Type, Date, Text)
Publication 20001228 A1 With international search report.
Examination 20010802 Request for preliminary examination prior to end of 19th month from priority date
Fulltext Availability:
Claims

Claim
... I 00 Name
@-- SourceServerll)
I 00 DestinationServerlD Protocol
51 co Description
TrustDefID
I P Type
Port
-1713
---------- Proxied
ProxyDefID
Addressable Reso
Encrypted
---------- Details
If ,Pre-defined
1 715
AuthenticationlD
Label
Authentication
ITrustlinayption Strength ----------
EncryptionlD iDescription...server to its ServerlD.
DBIPAndTypeByServerlDFile Relates servers to their locations inside or outside to the **VPN** . Maps ServerlD to the server's IP address and a flag indicating whether the address is inside or outside the **VPN** .
DBServicelDByPortFile Relates services to their **port numbers** . Maps from Servicell) to **port number** . DBServicelDByServerlDFile Relates servers to ports for services. Maps from ServerID to a list of **port numbers** . DBServicePodToProxyPorlFile Relates service pods to the ports for their proxies. Maps from service pod **number** to proxy **port number** . DBProxylDByServerlDFile Relates servers to service proxies. Maps from ServerlD to ProxyDeflD. DBProxyParametersFile Relates proxies to **configuration data** for the proxies.

11/5,K/19 (Item 15 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT

00764556 **Image available**
POLICY BASED NETWORK ARCHITECTURE
ARCHITECTURE DE RESEAU BASEE SUR UNE POLITIQUE
Legal Representative:
CHANG Josephine E (agent), Christie, Parker & Hale, LLP, 350 W. Colorado Boulevard, P.O. Box 7068, Pasadena, CA 91109-7068, US,
Patent and Priority Information (Country, Number, Date):
Patent: WO 200078004 A2-A3 20001221 (WO 0078004)
Application: WO 2000US16246 20000612 (PCT/WO US0016246)
Priority Application: US 99138849 19990610; US 99138850 19990610; US 99139033 19990610; US 99139034 19990610; US 99139035 19990610; US 99139036 19990610; US 99139038 19990610; US 99139042 19990610; US 99139043 19990610; US 99139044 19990610; US 99139047 19990610; US 99139048 19990610; US 99139049 19990610; US 99139052 19990610; US 99139053 19990610; US 99139076 19990611
Designated States: AU CN JP
(EP) AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE
Main International Patent Class: H04L-029/06
Publication Language: English
Filing Language: English
Fulltext Availability:
Detailed Description
Claims
Fulltext Word Count: 12303

English Abstract
A unified policy management system for an organization including a central policy server and remotely situated policy enforcers. A central database and policy enforcer databases storing policy settings are configured as LDAP databases adhering to a hierarchical object oriented structure. Such structure allows the policy settings to be defined in an intuitive and extensible fashion. Changes in the policy settings made at the central policy server are automatically transferred to the policy enforcers for updating their respective databases. Each policy enforcer collects and transmits health and status information in a predefined log format and transmits it to the policy server for efficient monitoring by the policy server. For further efficiencies, the policy enforcement functionalities of the policy enforcers are effectively partitioned so as to be readily implemented in hardware. The system also provides for dynamically routed VPNs where VPN membership lists are automatically created and shared with the member policy enforcers. Updates to such membership lists are also automatically transferred to remote VPN clients. The system further provides for fine grain access control of the traffic in the VPN by allowing definition of firewall rules within the VPN. In addition, policy server and policy enforcers may be configured for high availability by maintaining a backup unit in addition to a primary unit. The backup unit become active upon failure of the primary unit.

French Abstract
L'invention concerne un systeme unifie de gestion de politiques pour une organisation comprenant un serveur central de politiques et des organes d'execution de politique situes a distance. Une base de donnees centrale et des bases de donnees d'organes d'execution de politique stockant des parametres de politiques sont configurees comme des bases de donnees de protocoles LDAP soumises a une structure hierarchique orientee objet. Cette structure permet de definir les parametres de politique de maniere intuitive et extensible. Des modifications apportees a des parametres de politique au serveur central de politique sont transferees automatiquement aux organes d'execution de politique en vue d'une mise a jour de leurs bases de donnees respectives. Chaque organe d'execution de politique reunit des informations d'etat et de sante dans un format de journal predefini et les transmet au serveur de politiques pour permettre a celui-ci d'operer une surveillance efficace. Pour plus d'efficacite,

les fonctionnalites d'execution de politique des organes d'execution de politique sont divisees efficacement de maniere a pouvoir etre mises en place facilement dans le materiel. Le systeme prevoit egalement le routage dynamique de RPV, les listes des membres de RPV etant automatiquement creees et partagees avec les organes d'execution de politique membres. Les mises a jour de ces listes de membres sont egalement transferees automatiquement aux clients de RPV a distance. Le systeme assure en outre un controle d'acces a grain fin du trafic dans le RPV en permettant une definition de regles de pare-feu dans le RPV. De plus, on peut configurer le serveur de politiques et les organes d'execution de politique en vue d'une disponibilite elevee en maintenant une unite de reserve en plus de l'unite primaire. L'unite de reserve s'active lors d'une defaillance de l'unite primaire.

Legal Status (Type, Date, Text)
Publication 20001221 A2 Without international search report and to be republished upon receipt of that report.
Search Rpt 20010830 Late publication of international search report
Republication 20010830 A3 With international search report.

Fulltext Availability:
Claims
Claim
... the creation of dynamically routed VPNs where VPN membership lists are automatically created without statically **configuring** the membership **information** by the network administrator. Thus, once the administrator configures a **VPN** from one policy enforcer's LAN to another, routing 1 5 protocols such as RIPv1...

...interfaces learn about the networks reachable through their respective interfaces. These networks then become the **VPN** 's members, and the policy enforcers 124, 126 on either side of the **VPN** create membership tables using the learned routes. The membership information is preferably exchanged between the...

...132, 134. Thus, the combined use of routing protocols and LDAP allows the creation of **VPNs** whose member lists are dynamically compiled. Referring again to FIG. 8, the network administrator configures **VPN** policies for multiple site connectivity using the resource palette 718 and policy canvas 720. Selection of the **VPN** tab 720b in the policy canvas 720 causes the display of a collection of **VPN** clouds 270 already configured for the system as is illustrated in FIG. 13. As described above, a **VPN** cloud is an individual **VPN** or a group of **VPNs** for which a security policy may be defined. Each **VPN** cloud includes a list of sites under a sites node 234 and users under a...

...of the policy enforcers 124, 126. The policy enforcers for the sites preferably act as **VPN** **tunnel** endpoints once the hosts under the sites start communicating. The users in the **VPN** cloud are the users who may access the hosts associated with the sites 234. The users access the hosts as **VPN** clients using **VPN** client software installed in each user's personal computer as is described in further detail below. Each **VPN** cloud 270 further includes a **firewall** rules node 276 including **firewall** rules to be applied all the connections in the cloud. The rules may govern, among other things, **VPN** 3) 5 access permissions, security features such as the level of encryption and authentication used for the connectivity at the network layer.

11/5,CM/35 (Item 31 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT

00427785
OUTSIDE ACCESS TO COMPUTER RESOURCES THROUGH A FIREWALL
ACCES DEPUIS L'EXTERIEUR A DES RESSOURCES INFORMATIQUES AU TRAVERS D'UN DISPOSITIF DE REMPART
Patent and Priority Information (Country, Number, Date):
Patent: WO 9818248 A1 19980430
Application: WO 97GB2712 19971002 (PCT/WO GB9702712)
Priority Application: US 96731800 19961021
Designated States: BR CA CN CZ HU JP KR PL RU AT BE CH DE DK ES FI FR GB GR IE IT LU MC NL PT SE
Main International Patent Class: H04L-029/06
Publication Language: English
Fulltext Availability:
Claims
Fulltext Word Count: 3866

English Abstract
A firewall isolates computer and network resources inside the firewall from networks, computers and computer applications outside the firewall. Usually, a firewall allows for an inside user or object to originate connection to an outside object or network, but does not allow for connections to be generated in the reverse direction; i.e. from outside in. The disclosed invention provides a special "tunnelling" mechanism, operating on both sides of a firewall, for establishing such "outside in" connections when they are requested by certain "trusted" individuals or objects or applications outside the firewall. The mechanism includes special tunnelling applications, running on interface servers inside and outside the firewall, and a special table of "trusted sockets" created and maintained by the inside tunnelling application.

French Abstract
Un dispositif de rempart isole les ressources informatiques et les ressources du reseau, lesquelles se trouvent a l'interieur du perimetre protege par le rempart, des reseaux, ordinateurs et applications informatiques se trouvant de l'autre cote du rempart. En general, un dispositif de rempart permet a un utilisateur ou un objet interne d'etablir une connexion avec un objet ou un reseau externe, mais ne permet pas les connexions en sens inverse, c'est-a-dire les connexions s'etablissant de l'exterieur vers l'interieur. La presente invention concerne un mecanisme de "tunnel" particulier fonctionnant des deux cotes d'un dispositif de rempart et permettant d'etablir des connexions depuis l'exterieur lorsque ces dernieres sont demandees par certaines personnes, objets ou applications "de confiance" se trouvant a l'exterieur du perimetre protege par le dispositif de rempart. Ledit mecanisme comprend des applications de tunnel particulieres qui s'executent sur des serveurs d'interface se trouvant a l'interieur et a l'exterieur du perimetre protege par le dispositif de rempart, ainsi qu'une table particuliere de "prises securisees" creees et entretenues par l'application de tunnel interne.

Claim
1 **Tunnelling** apparatus for a **data** communication network containing a **firewall** (1), said **firewall** defining inside and outside regions and forming a security barrier preventing objects in said outside region from directly initiating access to objects in said inside region, while permitting objects in said inside region to directly initiate and obtain access to objects in said outside region; said **tunnelling** apparatus comprising:
an outside interface computer (3) in said outside region, said outside interface computer interfacing between said **firewall** (1) and objects in said outside region;
an inside interface computer (2) in said inside region, said inside interface computer interfacing between said **firewall** (1) and objects in said inside region;

means in both said inside and outside interface computers for ascertaining identities of predetermined trusted objects in said inside region to which access is allowed from said outside region;
means in said outside interface computer, responsive to a request sent from an object in said outside region, for cooperating with said ascertaining means to determine if that request is directed to one of said
trusted objects and, if the request is so directed, for routing the request to said inside interface computer; and
means in both said inside and outside interface computers responsive to said request directed to said one of said trusted object for forming a data communication connection between said one of said trusted objects and
the outside object that sent the respective request; wherein segments of said data communication connection located in said inside region and extending through said **firewall** are formed under exclusive control of said
inside interface computer, and a segment of said data communication connection extending from said outside interface computer to the object that sent the request is formed under control of said outside interface computer.

13/5,K/1 (Item 1 from file: 348)
DIALOG(R)File 348:EUROPEAN PATENTS

01361300
System and method for secure duplex browser communication over disparate networks
System und Verfahren zur gesicherte duplex Browserskommunikation uber unterschiedliche Netzwerke
Procede et systeme de communication duplex securisee entre navigateurs sur des reseaux heterogenes
PATENT ASSIGNEE:
Attachmate Corporation, (2738680), 3617 131th Avenue SE, Bellevue, Washington 98006, (US), (Applicant designated States: all)
INVENTOR:
Hardwick, Brian Keith, 4413 State Route 46, West Harrison, Indiana 47060, (US)
Towne, Calvin David, 209 E 3rd Street, Franklin, Ohio 45005, (US)
LEGAL REPRESENTATIVE:
Grunecker, Kinkeldey, Stockmair & Schwanhausser Anwaltssozietat (100721), Maximilianstrasse 58, 80538 Munchen, (DE)
PATENT (CC, No, Kind, Date): EP 1161048 A2 011205 (Basic)
APPLICATION (CC, No, Date): EP 2001111875 010516;
PRIORITY (CC, No, Date): US 575330 000519
DESIGNATED STATES: AT; BE; CH; CY; DE; DK; ES; FI; FR; GB; GR; IE; IT; LI; LU; MC; NL; PT; SE; TR
EXTENDED DESIGNATED STATES: AL; LT; LV; MK; RO; SI
INTERNATIONAL PATENT CLASS: H04L-029/06

ABSTRACT EP 1161048 A2
A system and method for secure duplex browser communication over disparate networks provides duplex communication between applications such as a browser program running on a client computer system and server applications running on a server computer system. Standard web-based protocols used with the duplex communication allow use of built-in browser program features such as related to security and navigation that would otherwise be specially provided. Given the request-response nature of many of the standard web-based protocols, use of standard web-based protocols for duplex communication has not been readily attainable in the past. A duplex transport system to provide the duplex communication includes a client component running on the client computer system and a server component running on the server computer system. The browser program controls one or more browser applications configured to run on the client computer system. One or more instances of the client component and one or more instances of the server component are run to form one or more sessions each having session identifiers. Each session has one or more data pipes, which are sub-sessions. A particular data pipe has a pipe identifier and provides two independent data paths of duplex data traffic between the browser applications that are communicatively linked to the instance of the client component and the server applications communicatively linked to the instance of the server component that are both associated with the respective session of the particular data pipe. Messages of the duplex data traffic contain both session and data pipe identifiers.
ABSTRACT WORD COUNT: 251
NOTE:
Figure number on first page: 2

LEGAL STATUS (Type, Pub Date, Kind, Text):
Application: 011205 A2 Published application without search report
LANGUAGE (Publication,Procedural,Application): English; English; English
FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS A	(English)	200149	3106
SPEC A	(English)	200149	5213
Total word count - document A			8319
Total word count - document B			0
Total word count - documents A + B			8319

...SPECIFICATION as firewall/proxy navigation features of HTTP including the proxy configuration of the browser, HTTP **authentication** , Internet security features of associated protocols such as Secure **Sockets** Layer/Transport Layer Security (**SSL** /TLS), and access to client certificates such as used in **SSL** /TLS. As a result, additional client code must be downloaded and configured to compensate for...

...download times are substantially increased. Management issues are also complicated when many different client network **configurations** are being supported. **Security** issues are also made more difficult such as when access to client certificates requires platform...

13/5,K/4 (Item 2 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT

00830867 **Image available**

ARCHITECTURE OF A BRIDGE BETWEEN A NON-IP NETWORK AND THE WEB
ARCHITECTURE D'UN PONT ENTRE UN RESEAU NON IP ET LE WEB

Patent Applicant/Assignee:
KONINKLIJKE PHILIPS ELECTRONICS N V, Groenewoudseweg 1, NL-5621 BA Eindhoven, NL, NL (Residence), NL (Nationality)
Inventor(s):
CHENG Doreen Y, Prof. Holstlaan 6, NL-5656 AA Eindhoven, NL,
Legal Representative:
DE JONG Durk J (agent), Internationaal Octrooibureau B.V., Prof. Holstlaan 6, NL-5656 AA Eindhoven, NL,

Patent and Priority Information (Country, Number, Date):
Patent: WO 200163874 A2-A3 20010830 (WO 0163874)
Application: WO 2001EP1880 20010220 (PCT/WO EP0101880)
Priority Application: US 2000184310 20000223; US 2000736069 20001213
Designated States: CN JP
(EP) AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE TR
Main International Patent Class: H04L-012/28
International Patent Class: H04L-012/66; H04L-029/06
Publication Language: English
Filing Language: English
Fulltext Availability:
Detailed Description
Claims
Fulltext Word Count: 6879

English Abstract
Thin glue layers bridge a Non-IP network and the Internet Web. Existing services in both networks are used directly wherever feasible, thereby achieving simplicity and efficiency. A Non-IP-specific application can use a Non-IP API to access Internet services, and an IP-based Internet browser can use commands encoded in HTTP, XML, Java, or proprietary formats to access Non-IP services and to control Non-IP devices. In this manner, changes are not required to the Internet browser. The glue layers translate between the IP protocol and Non-IP API, but also allow commands and responses to tunnel between end applications in the Internet and the Non-IP network without interpretation.

French Abstract
De fines couches "collantes" servent de pont entre un reseau non IP et le Web. Dans la mesure du possible, on utilise directement les services existant dans les deux reseaux, ce qui assure une plus grande simplicite et une efficacite plus elevee. Une application non specifique a l'IP peut utiliser une API non IP pour acceder aux services Internet, et un navigateur base sur le protocole IP peut utiliser les commandes codees en HTTP, XML, Java ou au format de proprietaires afin d'acceder aux services non IP et commander des dispositifs non IP. De cette maniere, aucune modification du navigateur Internet n'est requise. Les couches "collantes" effectuent la traduction entre le protocole IP et une API non IP et permettent aussi aux commandes et reponses de passer par un "tunnel" entre les applications finales de l'Internet et un reseau non IP sans interpretation.

Legal Status (Type, Date, Text)
Publication 20010830 A2 Without international search report and to be republished upon receipt of that report.
Search Rpt 20020124 Late publication of international search report
Republication 20020124 A3 With international search report.
Republication 20020124 A3 Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.

Fulltext Availability:
Detailed Description

Detailed Description
... of a HAVi object 240, 250.

The server 350 in a preferred embodiment is also **configured** to provide **security** . For example, if only **authorized** users can access the server, or if different users have different access rights, the server...

...the system allows access from outside the physical security area of the HAVI network, a **firewall** security system may be used. These and other security methods are common in the art, and include, for example, facilities such as **SSL** (Secure **Socket** Layer).

13/5,K/8 (Item 6 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT

00798275 **Image available**

SECURED SESSION SEQUENCING PROXY SYSTEM SUPPORTING MULTIPLE APPLICATIONS AND METHOD THEREFOR

SYSTEME MANDATAIRE DE SEQUENCAGE DE SESSION PROTEGEE ACCEPTANT PLUSIEURS APPLICATIONS ET METHODE AFFERENTE

Patent Applicant/Assignee:
THE CHASE MANHATTAN BANK, 270 Park Avenue, 41st Floor, New York, NY 10017, US, US (Residence), US (Nationality)
Inventor(s):
YARBOROUGH William J, 510 Cranes Way #107, Altamonte Springs, FL 32701, US,
Legal Representative:
WEISBURD Steven I (et al) (agent), Ostrolenk, Faber, Gerb & Soffen, LLP, 1180 Avenue of the Americas, New York, NY 10036, US,

Patent and Priority Information (Country, Number, Date):
Patent: WO 200131874 A2-A3 20010503 (WO 0131874)
Application: WO 2000US29836 20001030 (PCT/WO US0029836)
Priority Application: US 99162003 19991028
Designated States: AE AG AL AM AT AU AZ BA BB BG BR BY CA CH CN CR CU CZ DE DK DM DZ EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT TZ UA UG UZ VN YU ZA ZW
(EP) AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE
(OA) BF BJ CF CG CI CM GA GN GW ML MR NE SN TD TG
(AP) GH GM KE LS MW MZ SD SL SZ TZ UG ZW
(EA) AM AZ BY KG KZ MD RU TJ TM
Main International Patent Class: H04L-029/06
Publication Language: English
Filing Language: English
Fulltext Availability:
Detailed Description
Claims
Fulltext Word Count: 10852

English Abstract
A security system controls communications between one or more client systems and one or more hosts. Each host provides one or more services which can be accessed by one or more client systems. The security system includes a server having a plurality of server sockets. Each of the server sockets corresponds to a different one of the services such that there is a one to one correspondence between the server sockets and the services provided by the hosts. A firewall is coupled between the client systems and the server and receives a plurality of requests for different ones of the services over a first socket on the firewall such that there is a many to one correspondence between the services and the first socket on the firewall. One or more software modules examine each respective one of the requests for service received on the first socket of the firewall and causes it to be forwarded to that socket on the server which corresponds to the service requested.

French Abstract
Ce systeme de securite agit sur des communications entre un ou plusieurs systemes clients et un ou plusieurs hotes. Chaque hote fournit un ou plusieurs services auxquels un ou plusieurs systemes clients peuvent acceder. Ce systeme de securite comporte un serveur possedant plusieurs ports de serveur. Chacun de ces ports correspond a l'un des services, de sorte qu'il y a correspondance biunivoque entre les ports et les services fournis par les hotes. Un pare-feu est installe entre les systemes clients et le serveur et un premier port de ce pare-feu recoit plusieurs demandes relatives aux divers services, de sorte qu'il y a correspondance multiunivoque entre les services et le premier port du pare-feu. Un ou plusieurs modules de logiciel examinent chacune des demandes de service le premier port du pare-feu et acheminent cette demande vers le port du serveur correspondant au service demande.

Legal Status (Type, Date, Text)
Publication 20010503 A2 Without international search report and to be republished upon receipt of that report.
Examination 20010823 Request for preliminary examination prior to end of 19th month from priority date
Search Rpt 20020124 Late publication of international search report
Republication 20020124 A3 With international search report.

Fulltext Availability:
Detailed Description

Detailed Description
... data contained
in the configuration file. One category of data contains values identifying the (three) **sockets** on the external **firewall** 16. A second category **identifies** the multitude of **sockets** on public proxy server 18, each of which corresponds with a respective service provided by hosts 4. A third category of **data** in **configuration** file comprises directives for the types of encryption methods to be used.
During the course...

13/5,K/19 (Item 17 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT

00484747
SECURE CUSTOMER INTERFACE FOR WEB-BASED DATA MANAGEMENT
INTERFACE UTILISATEUR SECURISEE POUR LA GESTION DE DONNEES SUR LE WEB
Patent Applicant/Assignee:
DEVINE Carol Y,
SHIFRIN Gerald A,
SHOULBERG Richard W,
Inventor(s):
DEVINE Carol Y,
SHIFRIN Gerald A,
SHOULBERG Richard W,
Patent and Priority Information (Country, Number, Date):
Patent: WO 9916099 A2 19990401
Application: WO 98US20158 19980925 (PCT/WO US9820158)
Priority Application: US 9760655 19970926
Designated States: AU BR CA JP MX SG AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE
Main International Patent Class: H01J-013/00
Publication Language: English
Fulltext Availability:
Detailed Description
Claims
Fulltext Word Count: 16305

English Abstract
An integrated series of security protocols is disclosed that protect remote user communications (22) with remote enterprise services, and simultaneously protect the enterprises services from third parties. In the first layer, an implementation of the Secure Sockets Layer (SSL) version of a HTTPS provides communications security, including authentication of the enterprise web server and the security of the transmitted data. The protocols provide for an identification of the user, and an authentication of the user to ensure the user is who he/she claims to be and a determination of entitlements that the user may avail themselves of within the enterprise system. Session security is described, particularly as to the differences between a remote user's copper wire connection to a legacy system and a user's remote connection to the enterprise system over a "stateless" public Internet (15), where each session is a single transmission, rather than an interval of time between logon and logoff, as is customary in legacy systems. Security for

the enterprise network and security for the data maintained by the various enterprise applications is also described.

French Abstract

Cette invention decrit une serie integree de protocoles de securite qui protegent des communications d'utilisateurs distants etablies avec des services d'entreprises distantes, et qui protegent simultanement les services d'entreprises contre tout acces par des tiers. Dans la premiere couche, une execution de la version SSL (couche ports d'acces securises) du protocole HTTPS assure la securite des communications, y compris l'authentification du serveur Web de l'entreprise et la securite des donnees transmises. Ces protocoles fournissent une identification de l'utilisateur et une authentification de l'utilisateur, pour assurer que l'utilisateur est bien la personne qu'il pretend etre, ainsi qu'une determination des autorisations dont l'utilisateur peut se prevaloir lui-meme a l'interieur du systeme de l'entreprise. La securite des sessions est decrite, en particulier en rapport avec les differences entre une connexion fil de cuivre d'un utilisateur distant avec un systeme legue et une connexion distante d'un utilisateur avec le systeme de l'entreprise par l'intermediaire d'un reseau public "apatride" comme l'Internet, dans lequel chaque session constitue une transmission unique, plutot qu'un intervalle de temps entre une ouverture de session et une fermeture de session, comme c'est le cas d'habitude dans les systemes legues. La securite du reseau de l'entreprise et la securite des donnees conservees par les diverses applications de l'entreprise sont egalement decrites.

Fulltext Availability:
Detailed Description
Claims

Detailed Description
... corporate Intranet 30. The messaging sent to the Dispatcher Server 26 will include the user **identifier** and **session information** , the target proxy **identifier** , and the proxy specific data. The decode/dispatcher server 26 then **authenticates** the user's access to the desired middle-tier service from cached data previously received...

...the StarOE server as will be hereinafter described in greater detail in connection with User **Identification** and **Authentication** .

As shown in Figure 4, the Secure Web server 24 forwards the Dispatcher header and...

Claim
... communication between said client browser and said secure web server, said secure server also providing **session** management including client **identification** , **validation** and **session** management to link said session with said client:
(c) at least one dispatcher server for communicating with said secure web server through a first **firewall** , and communicating with a plurality of proxy services and system resources using an internal network, said dispatcher server providing **verification** of system access after client entitlements have been **verified** ;
(d) said plurality of system resources providing communications network management capabilities for said client, each...

13/5,K/24 (Item 22 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT

00376168

SECURED GATEWAY INTERFACE

INTERFACE INTER-RESEAU SECURITAIRE

Patent Applicant/Assignee:
INTERNATIONAL BUSINESS MACHINES CORPORATION,
IBM UNITED KINGDOM LIMITED,

Inventor(s):
GORE Robert Cecil,
HAUGH John Frederick,

Patent and Priority Information (Country, Number, Date):
Patent: WO 9716911 A1 19970509
Application: WO 96GB664 19960320 (PCT/WO GB9600664)
Priority Application: US 95551260 19951031

Designated States: BR CA CN CZ HU JP KR PL RU AT BE CH DE DK ES FI FR GB GR IE IT LU MC NL PT SE

Main International Patent Class: H04L-029/06

Publication Language: English

Fulltext Availability:
Detailed Description
Claims

Fulltext Word Count: 5892

English Abstract

A computer implemented method, uniquely programmed computer system, and article of manufacture embodying a computer readable program means allow a customer on an external network (310) to initiate an authorized business transaction utilizing internal business resources (330) on an internal network (320) without violating security firewalls (300). Specifically, the method directs an internal computer system (320) to allow an external computer system (310) to initiate a transaction request (2) using internal resources (330) without violating a security firewall (300) between the internal computer system (320) and the external computer system (310). The method includes a first step of authenticating a connection initiated by the internal computer system (320) between the internal computer system (320) and the external computer system (310), thereby establishing an authenticated connection. The second step includes calling by the external computer system (310) a transaction request (2) received by the external computer system (310). In response to calling the transaction request (2), the third step includes creating by the external computer system (310) a string comprising the transaction request (2), arguments, and process environment variables for executing the transaction request (2). The fourth step includes transmitting by the external computer system (310) the string to the internal computer system (320) through the authenticated connection. The fifth step includes verifying by the internal computer system (320) the transaction request (2). The sixth step includes recreating by the internal computer system (320) the original process environment. The final step includes executing by the internal computer system (320) the transaction request (2), thereby generating an output.

French Abstract

On decrit un procede mis en oeuvre par un ordinateur, un systeme d'ordinateur programme de maniere unique, ainsi qu'un produit manufacture reunissant un programme lisible par un ordinateur, lesquels permettent a un client se situant sur un reseau externe (310) de demarrer, sur un reseau interne (320), une transaction commerciale autorisee a l'aide de ressources commerciales internes (330), sans violer des filtres securitaires (300). Plus precisement, le procede dirige un systeme informatique interne (320), afin de permettre a un systeme informatique externe (310) de demarrer une demande (2) de transaction en utilisant des ressources internes (330), sans violer un filtre securitaire (300) place entre le systeme interne (320) et le systeme externe (310). Ce procede comprend une premiere etape consistant a authentifier une connexion demarree par le systeme informatique interne (320), entre celui-ci (320) et le systeme informatique externe (310), etablissant ainsi une connexion authentifiee. La seconde etape consiste en l'appel par le systeme informatique externe (310) d'une demande (2) de transaction recue par ce systeme externe (310). En reponse a cet appel de demande (2) de

transaction, la troisieme etape consiste en la creation par le systeme externe (310) d'une chaine comprenant la demande (2) de transaction, des arguments, ainsi que des variables d'environnement de procede, aux fins d'execution de cette demande (2). La quatrieme etape comprend la transmission de la chaine, par le systeme externe (310) et vers le systeme interne (320), via la connexion authentifiee. La cinquieme etape comprend la verification par le systeme interne (320) de la demande (2) de transaction. La sixieme etape comprend une nouvelle creation, par le systeme interne (320), de l'environnement du procede originel. L'etape finale comprend l'execution par le systeme interne (320) de la demande (2) de transaction, avec pour consequence la production d'une sortie.

Fulltext Availability:
Detailed Description

Detailed Description
... file
and stores a table of valid services in memory, creates a socket on the **identified** communication **port** , and finally generates a standard connect
call at 450 across **firewall** 300 to outside daemon 312, which is listening
at 430. Because the connection is being initiated from an internal server, **firewall** 300 **permits** the connection.

```
File 238:Abs. in New Tech & Eng. 1981-2002/Jan
         (c) 2002 Reed-Elsevier (UK) Ltd.
File 108:AEROSPACE DATABASE 1962-2001/DEC
         (c) 2002 AIAA
File   8:Ei Compendex(R) 1970-2002/Jan W4
         (c) 2002 Engineering Info. Inc.
File  77:Conference Papers Index 1973-2002/Jan
         (c) 2002 Cambridge Sci Abs
File  35:Dissertation Abs Online 1861-2002/Jan
         (c) 2002 ProQuest Info&Learning
File 202:Information Science Abs. 1966-2002/ISSUE 01
         (c) Information Today, Inc
File  65:Inside Conferences 1993-2002/Jan W4
         (c) 2002 BLDSC all rts. reserv.
File   2:INSPEC 1969-2002/Jan W4
         (c) 2002 Institution of Electrical Engineers
File  14:Mechanical Engineering Abs 1973-2002/Jan
         (c) 2002 Cambridge Sci Abs
File 233:Internet & Personal Comp. Abs. 1981-2002/Feb
         (c) 2002 Info. Today Inc.
File  94:JICST-EPlus 1985-2002/Dec W3
         (c)2002 Japan Science and Tech Corp(JST)
File 111:TGG Natl.Newspaper Index(SM) 1979-2002/Jan 29
         (c) 2002 The Gale Group
File 603:Newspaper Abstracts 1984-1988
         (c)2001 ProQuest Info&Learning
File 483:Newspaper Abs Daily 1986-2002/Jan 28
         (c) 2002 ProQuest Info&Learning
File   6:NTIS 1964-2002/Feb W2
         (c) 2002 NTIS, Intl Cpyrght All Rights Res
File 144:Pascal 1973-2002/Jan W4
         (c) 2002 INIST/CNRS
File 434:SciSearch(R) Cited Ref Sci 1974-1989/Dec
         (c) 1998 Inst for Sci Info
File  34:SciSearch(R) Cited Ref Sci 1990-2002/Jan W4
         (c) 2002 Inst for Sci Info
File  99:Wilson Appl. Sci & Tech Abs 1983-2001/Dec
         (c) 2002 The HW Wilson Co.
File 583:Gale Group Globalbase(TM) 1986-2002/Jan 28
         (c) 2002 The Gale Group
File 266:FEDRIP 2002/Dec
         Comp & dist by NTIS, Intl Copyright All Rights Res
File  62:SPIN(R) 1975-2002/Jan W2
         (c) 2002 American Institute of Physics
File 438:Library Literature 1984-2001/Dec
         (c) 2002 The HW Wilson Co
File  61:LISA(LIBRARY&INFOSCI) 1969-2002/Jan
         (c) 2002 Reed Reference Publishing

Set     Items   Description
S1       5273   FIREWALL? ? OR (BASTION OR PROXY)()HOST? ? OR APPLICATION(-
                )(GATEWAY? ? OR GUARD? ?)
S2     481553   TUNNEL? OR VIRTUAL()PRIVATE()NETWORK? OR VPN OR VPNS
S3    4774484   AUTHENTICAT? OR VERIF? OR VALIDAT? OR IDENTIF? OR SCREEN???
               OR CHECK??? OR AUTHORIZ? OR AUTHORIS? OR PERMIT? OR PERMISSI-
              ON
S4      16300   SOCKET? ? OR WINSOCK OR SSL
S5    4492420   OBJECT? ? OR CLASS?? OR INHERITANCE OR JAVA OR APPLET? ? OR
               COMPONENT? ?
S6      33977   (CONFIGUR? OR TUNNEL?)(3N)(DATA OR INFORMATION) OR PORT? ?-
              (3N)(NUMBER? OR ADDRESS? OR ID OR IDENTIF???? OR IDENTIFICATI-
              ON) OR SESSION? ?(3N)(ID OR IDENTIF???? OR IDENTIFICATION OR -
              DATA OR INFORMATION) OR (SECURITY OR TUNNEL?)(5N)CONFIGUR?
S7          1   S1 AND S2 AND S4 AND S6
S8          5   S2 AND S4 AND S6
S9         28   S1 AND S2 AND S4
S10        25   RD (unique items)
S11        29   S8 OR S10
```

S12	336	S1 AND S2 AND S3
S13	31	S1 AND S2 AND S6
S14	27	RD (unique items)
S15	26	S14 NOT S11

11/5/3 (Item 2 from file: 8)
DIALOG(R)File 8:Ei Compendex(R)

05133240 E.I. No: EIP98104408721
Title: Internet/Intranet firewall security - policy, architecture and transaction services
Author: Hunt, Ray
Corporate Source: Univ of Canterbury, Christchurch, New Zealand
Source: Computer Communications v 21 n 13 Sep 1 1998. p 1107-1123
Publication Year: 1998
CODEN: COCOD7 ISSN: 0140-3664
Language: English
Document Type: JA; (Journal Article) Treatment: T; (Theoretical)
Journal Announcement: 9812W1
Abstract: The development of Internet/Intranet security is of paramount importance to organizations that plan to gain the economic benefits from interconnection with the Internet. This paper commences by examining **firewall** policy, focusing on both network service access policy and **firewall** design policy. Various **firewall** architectures, ranging from simple packet filters through to screened subnets and proxy gateways, are then discussed. Finally, the various mechanisms by which transactions can be secured over the Internet/Intranet are covered. These include encrypted **tunnelling** , IPv6, point-to-point **tunnelling** protocol, secure **sockets** layer, secure electronic transactions and secure multipart Internet mail encoding. (Author abstract) 21 Refs.
Descriptors: Security of data; Internet; Intranets; Computer system **firewalls** ; Computer architecture; Telecommunication services; Telecommunication control; Public policy; Computer systems programming; Digital filters
Identifiers: Internet/Intranet **firewall** security; Network service access policy; Packet filters; Screening routers; Dual-homed gateways; Proxy gateways
Classification Codes:
723.2 (Data Processing); 723.1 (Computer Programming)
723 (Computer Software); 722 (Computer Hardware); 716 (Radar, Radio & TV Electronic Equipment); 901 (Engineering Profession)
72 (COMPUTERS & DATA PROCESSING); 71 (ELECTRONICS & COMMUNICATIONS); 90 (GENERAL ENGINEERING)

11/5/4 (Item 3 from file: 8)
DIALOG(R)File 8:Ei Compendex(R)

04537324 E.I. No: EIP96100380068
Title: Strategic security
Author: Ranum, Marcus J.
Corporate Source: V-One Corp, Rockville, MD, USA
Source: Data Communications v 25 n 14 Oct 1996. 5pp
Publication Year: 1996
CODEN: DACODM
Language: English
Document Type: JA; (Journal Article) Treatment: G; (General Review)
Journal Announcement: 9612W4
Abstract: Essentially, there are three types of technologies used to build secure networks. Access-control products keep intruders off the corporate net. Secure payment schemes enable customers to conduct business safely over the Internet. Transaction technologies establish protected links to known partners. However, most security schemes do one thing well. Thus, net managers should mix and match the best technologies for the job. Furthermore, they also have to pay close to network design.
Descriptors: *Computer networks; Security of data; Information management ; Data communication systems; Network protocols; Cryptography; Computer software; Virtual reality; Information technology; Modems
Identifiers: Web servers; **Firewalls** ; Authentication servers; Secure **sockets** layer; Secure hypertext transfer protocol; **Virtual private network** ; Internet service provider; Cybercrooks; Remote access software;

Network security
Classification Codes:
722.3 (Data Communication, Equipment & Techniques); 723.2 (Data Processing); 716.1 (Information & Communication Theory); 723.1 (Computer Programming); 723.5 (Computer Applications)
722 (Computer Hardware); 723 (Computer Software); 716 (Radar, Radio & TV Electronic Equipment); 903 (Information Science)
72 (COMPUTERS & DATA PROCESSING); 71 (ELECTRONICS & COMMUNICATIONS); 90 (GENERAL ENGINEERING)

11/5/5 (Item 1 from file: 2)
DIALOG(R)File 2:INSPEC

6508835 INSPEC Abstract Number: C2000-04-6130S-005
Title: SSL **and TLS protocols: how to address critical security issues**
Author(s): Oppliger, R.
Journal: Computer Security Journal vol.16, no.1 p.15-38
Publisher: Comput. Security Inst,
Publication Date: Winter 2000 Country of Publication: USA
CODEN: CSJLDR ISSN: 0277-0865
SICI: 0277-0865(200024)16:1L.15:PACS;1-E
Material Identity Number: G684-2000-001
Language: English Document Type: Journal Paper (JP)
Treatment: Practical (P)
Abstract: **SSL** became the predominant protocol to provide security services for HTTP data traffic after 1994. The latest specification of **SSL** 3.0 was officially released in March 1996. It is implemented in both Netscape Navigator 3.0 (and higher) and Microsoft Internet Explorer 3.0 (and higher). **SSL** 3.0 has also been adapted by the IETF TLS WG. In fact, the TLS 1.0 protocol specification is a derivative of **SSL** 3.0. The article focuses only on the **SSL** and TLS protocols. It is concluded that the **SSL** and TLS protocols are well suited to provide communication security services for TCP based applications. In fact, the user community of the **SSL** and TLS protocols is growing very rapidly. There is a practical difficulty in **tunneling SSL** and TLS **data** traffic through a **firewall** (this difficulty is due to the fact that the **SSL** and TLS protocols are end-to-end protocols, and that any **firewall** represents a man-in-the-middle). Unfortunately, the protocols have two additional problems that are even more difficult to address: first, none of the two protocols (neither **SSL** nor TLS) provides a viable solution for the security-related problems of UDP based applications; second and more important, the deployment of **SSL** and TLS based solutions is seriously limited by the currently existing US export controls. (17 Refs)
Subfile: C
Descriptors: government policies; hypermedia; Internet; security of data; transport protocols
Identifiers: TLS protocols; critical security issues; security services; HTTP data traffic; **SSL** 3; Netscape Navigator 3; Microsoft Internet Explorer 3; IETF TLS WG; TLS 1; protocol specification; communication security services; TCP based applications; user community; data traffic; **firewall** ; end-to-end protocols; security-related problems; UDP based applications; US export controls
Class Codes: C6130S (Data security); C0310D (Computer installation management); C5640 (Protocols); C6130M (Multimedia); C6150N (Distributed systems software); C5620W (Other computer networks); C0230 (Economic, social and political aspects of computing)

11/5/6 (Item 2 from file: 2)
DIALOG(R)File 2:INSPEC

6455640 INSPEC Abstract Number: B2000-02-6210L-106, C2000-02-5620L-023
Title: VPN **products. Made in Russia**
Author(s): Gvozdev, I.M.; Zaichikov, V.N.; Moshak, N.N.; Pelenitsyn, M.B.

; Seleznev, S.P.; Shepelyavyi, D.A.
Author Affiliation: Bank of Russia, Moscow, Russia
Journal: Seti i Sistemy Svyazi no.12 p.102-12
Publisher: OOO-`Antonyuk-Konsalting',
Publication Date: 1 Oct. 1999 Country of Publication: Russia
CODEN: SSSVF8
Material Identity Number: G476-1999-014
Language: Russian Document Type: Journal Paper (JP)
Treatment: Practical (P); Product Review (R)
Abstract: Thirteen **VPN** (**virtual private network**) systems produced by Russian companies and meeting the requirements of the GOST 28147-89 state standard are considered. The performance, resources and advantages/disadvantages of the following systems are compared: FPSU-IP (Amikon Co.), IP-LIR (Infoteks Co.), Zastava (Elvis Plyus Co. and Ankad Co.), Ship/Verba (MO PNIEI Co.), Skip-MTsI/Verba (Ankei Co., MO PNIEI Co.), Pix **Firewall** (Cisco Systems Co.), Inter-Pro (Signal-Kom Co.), **SSL** -Baikonur (Ankad Co.), Fort/Verba-O Proxy (Ankei Co., MO PNIEI Co.), Net-Pro (Signal-Kom Co.), DataGuard/24S (Signal-Kom Co.), and FPSU-X.25 (Amikon Co.). (0 Refs)
Subfile: B C
Descriptors: Internet; LAN interconnection; telecommunication standards
Identifiers: **VPN** products; **virtual private network** ; GOST 28147-89 state standard; FPSU-IP; IP-LIR; Zastava; Ship/Verba; Skip-MTsI/Verba; Pix **Firewall** ; Inter-Pro; **SSL** -Baikonur; Fort/Verba-O Proxy; Net-Pro; DataGuard/24S; FPSU-X.25
Class Codes: B6210L (Computer communications); C5620L (Local area networks); C5620W (Other computer networks)

11/5/7 (Item 3 from file: 2)
DIALOG(R)File 2:INSPEC

6304725 INSPEC Abstract Number: B1999-09-6210L-021, C1999-09-5620W-020
Title: VPN **construction method for multiple** firewall **environment**
Author(s): Kayashima, M.; Terada, M.; Fujiyama, T.; Koizumi, M.; Katou, E.
Author Affiliation: Syst. Dev. Lab., Hitachi Ltd., Yokohama, Japan
Journal: Transactions of the Institute of Electronics, Information and Communication Engineers D-I vol.J82D-I, no.6 p.772-8
Publisher: Inst. Electron. Inf. & Commun. Eng,
Publication Date: June 1999 Country of Publication: Japan
CODEN: DTRDES ISSN: 0915-1915
SICI: 0915-1915(199906)J82DI:6L.772:CMMF;1-2
Material Identity Number: M972-1999-007
Language: Japanese Document Type: Journal Paper (JP)
Treatment: Practical (P)
Abstract: In the business field, the **VPN** (**virtual private network**) system, which is one of the construction methods for private networks over the Internet, is gaining prominence, but currently, the **VPN** architecture does not consider multiple **firewalls** , which creates some problems. We propose a "seamless **VPN** ", a new **VPN** construction method for a multiple **firewall** environment. It consists of a transport-layer gateway program on each **firewall** and a **socket** library for end-point clients. Each gateway has an end-to-end data encryption function and a relay-circuit setup function. Using these functions, the seamless **VPN** method is able to construct a **VPN** in a multiple **firewall** environment. (9 Refs)
Subfile: B C
Descriptors: authorisation; business communication; cryptography; Internet; transport protocols
Identifiers: **virtual private network** ; seamless **VPN** construction method; multiple **firewall** environment; Internet; transport-layer gateway program; **socket** library; end-point clients; end-to-end data encryption function; relay-circuit setup function
Class Codes: B6210L (Computer communications); B6150M (Protocols); B6120D (Cryptography); C5620W (Other computer networks); C6130S (Data security);

C7210N (Information networks); C5640 (Protocols)

11/5/8 (Item 1 from file: 233)
DIALOG(R)File 233:Internet & Personal Comp. Abs.

00642069 01PI09-125
A server appliance for the masses
Brown, Bruce; Brown, Marge
PC Magazine , September 25, 2001 , v20 n16 p46, 1 Page(s)
ISSN: 0888-8507
Company Name: Systemax
URL: http://www.systemax.com
Product Name: Systemax iMASS II
Languages: English
Document Type: Hardware Review
Grade (of Product Reviewed): B
Geographic Location: United States
Presents a favorable review of the Systemax iMASS II ($2,699), a versatile multipurpose network server appliance from Systemax Inc. of Port Washington, NY (800). Explains that it has automatic setup as well as easy hard drive backup and maintenance. Highlights its automated configuration, 1GHz Athlon processor, 128MB of RAM, two 10/100 network cards, integrated 56K modem, 40GB hard drive, 120GB second hard drive for data backup, and provision of File Transfer Protocol (FTP), e-mail, **virtual private network** (**VPN**), Remote Access Server (RAS), self-configuring **firewall** , and Web services with Secure **Sockets** Layer (**SSL**). Mentions, however, that it is unable to access an external **VPN** using Internet Protocol Security (IPSec). Concludes that it delivers value to small businesses. On a scale ranging from 1 to 5, received the rating of 4. Includes a photo. (MEM)
Descriptors: Network Server; Server; Network Computer; Multifunction Devices; Client-Server Computing; Network Security; Small Business
Identifiers: Systemax iMASS II; Systemax

11/5/10 (Item 3 from file: 233)
DIALOG(R)File 233:Internet & Personal Comp. Abs.

00636806 01NC07-106
Check Point next generation: Firewall **-1 gets a forklift**
Fratto, Mike
Network Computing , July 23, 2001 , v12 n15 p22-24, 2 Page(s)
ISSN: 1046-4468
Company Name: Check Point Software Technologies
URL: http://www.checkpoint.com
Product Name: **VPN** -1/ **Firewall** -1 Next Generation
Languages: English
Document Type: Software Review
Grade (of Product Reviewed): A
Geographic Location: United States
Presents a very favorable review of **VPN** -1/ **Firewall** -1 Next Generation ($3,495), **virtual private network** (**VPN**) and **firewall** software from Check Point Software Technologies (800, 650). Explains it offers a host of enhancements in management, policy development, SecureClient functionality, and redundancy. Highlights three additional views in the Visual Policy Editor that provide alternative methods for accessing objects, drag-and-drop functionality, ease of installation, internal certificate authority for interprocess security using client-side Secure **Sockets** Layer (**SSL**), ability to query the database for specific classes of objects by Internet Protocol (IP) address or subnet, centrally managed desktop firew and support of failover policy servers. Mentions no significa drawbacks. Concludes that Check Point has made enough improvement to make installing its **VPN** and **firewall** much more convenient. Includes a screen display. (MEM)

Descriptors: **Virtual Private Networks** ; **Firewalls** ; Network Security; Certificate Authorities; Encryption; Digital Certificates; Security Measures

Identifiers: **VPN** -1/ **Firewall** -1 Next Generation; Check Point Software Technologies

11/5/11 (Item 4 from file: 233)

DIALOG(R)File 233:Internet & Personal Comp. Abs.

00630746 01NC05-108

Buyer's guide: remote-office firewalls -- Firewalls **are an integral part of any remote-network plan. New features make them easier than ever to deploy**

Fratto, Mike

Network Computing , May 28, 2001 , v12 n11 p118-120, 3 Page(s)

ISSN: 1046-4468

Languages: English

Document Type: Articles, News & Columns

Geographic Location: United States

Presents guidelines designed to help information technology (IT) managers choose and deploy **firewalls** as part of a plan to support telecommuters or to move to broadband for remote offices. Cites features to look for: support of basic connectivity - 10/100Mbps ports, both client and server Dynamic Host Configuration Protocol (DHCP), local management, and Network Address Translation (NAT); built-in hub or switch; wireless access point; out-of-band management, such as serial port to which the IT team can connect a modem or terminal server just in case they need to make emergency repairs; egress filtering; **virtual private network** (**VPN**) gateway; manageability; support of Secure **Sockets** Layer (**SSL**); support of the Dynamic Domain Name System (DDNS) protocol that updates DNS records with current addressing information; and support of centralized logging. Includes a photo and a diagram. (MEM)

Descriptors: **Firewalls** ; Network Security; Telecommuting; Remote Computing; Broadband Communication; Security Measures; Client-Server Computing

11/5/12 (Item 5 from file: 233)

DIALOG(R)File 233:Internet & Personal Comp. Abs.

00630733 01NC05-005

Cisco's Pix firewall **line raises the price-performance ante**

Shipley, Greg

Network Computing , May 14, 2001 , v12 n10 p28-30, 2 Page(s)

ISSN: 1046-4468

Company Name: Cisco Systems

URL: http://www.cisco.com

Product Name: PIX 6.0 OS with PIX Device Manager

Languages: English

Document Type: Software Review

Grade (of Product Reviewed): A

Geographic Location: United States

Presents a very favorable review of PIX 6.0 OS with PIX Device Manager (free), **firewall** operating system from Cisco Systems Inc. (408). Explains that the PIX Device Manager is a Java-based graphical user interface (GUI) management console that allows for remote administration of the units over basic Hypertext Transfer Protocol (HTTP) with Secure **Sockets** Layer (**SSL**). Highlights the convenience of visual rule-set depiction without alienating those who prefer the command-line interface (CLI), state-based and nonstate-based failover capabilities, **virtual private network** (**VPN**) client, revamped documentation loaded with sample configurations, and unlimited session licensing. Mentions no significant drawbacks. Concludes that Cisco is making the right moves in the right direction with the PIX line of **firewalls** . Includes a screen display and a product summary. (MEM)

Descriptors: **Firewalls** ; Operating Systems; User Interface; Remote Computing; **Virtual Private Networks** ; Network Security; Client-Server Computing
Identifiers: PIX 6.0 OS with PIX Device Manager; Cisco Systems

11/5/13 (Item 6 from file: 233)
DIALOG(R)File 233:Internet & Personal Comp. Abs.

00627563 01NC04-101
One neck to choke -- Is the single-vendor solution right for you? Only if you demand accountability above all other aspects of your network management
Conover, Joel
Network Computing , April 16, 2001 , v12 n8 p52-62, 7 Page(s)
ISSN: 1046-4468
Languages: English
Document Type: Articles, News & Columns
Geographic Location: United States
Presents guidelines designed to help enterprise information technology (IT) managers choose single-vendor solutions in network management and Web management. Reports that an end-to-end solution in the enterprise means that a single vendor provides switching, routing, **firewall** , **virtual private network** (**VPN**), and wireless access while in the data center or collocation environment, it means the provision of Web load-balancing, caching, content-aware switching, and Secure **Sockets** Layer (**SSL**) termination and acceleration. Explains the benefits of partnering with one vendor: accountability, equipment support and maintenance, and customer leverage. Cites the need for the prospective customer to assess service and support costs and quality, gauge vendor culture, assess the fit of the company's product portfolio within the customer's enterprise. Includes three charts and three sidebars. (MEM)
Descriptors: Network Management; Web Management; Outsourcing; Contract

11/5/14 (Item 7 from file: 233)
DIALOG(R)File 233:Internet & Personal Comp. Abs.

00618808 01NC01-102
PrivateArk lets admins keep a tight rein on data
Raatz, Ben
Network Computing , January 22, 2001 , v12 n2 p30-32, 2 Page(s)
ISSN: 1046-4468
Company Name: Cyber-Ark Software
URL: http://www.cyber-ark.com
Product Name: PrivateArk 1.4
Languages: English
Document Type: Hardware Review
Grade (of Product Reviewed): B
Geographic Location: United States
Presents a favorable review of the PrivateArk 1.4 ($10,000), a network security server appliance from Cyber-Ark Software (888, 781). Explains that it provides end-to-end security for sharing data over a local area network (LAN), wide area network (WAN), or Internet. Highlights its **virtual private network** (**VPN**), **firewall** , file-access control, encryption and decryption on the client side, multiple methods of authentication including public key infrastructure and password-based challenge-response protocol, eas of installation, support of Secure **Sockets** Layer (**SSL**), and net masking. Mentions, however, that an activity log at the server console does not track password changes, permissions, authent methods, or group membership. Concludes that it is a strong soluti that enables enterprises to securely share data between departm or with other organizations. Includes a screen display and a product summary. (MEM)
Descriptors: Network Security; Security Measures; Network Server; **Virtual Private Networks** ; **Firewalls** ; Encryption; Public Key

Infrastructure
Identifiers: PrivateArk 1.4; Cyber-Ark Software

11/5/15 (Item 8 from file: 233)
DIALOG(R)File 233:Internet & Personal Comp. Abs.

00616269 00IY12-102
Uninvited guests -- For Web companies, security means opening their doors without giving away the business
Conour, Dale
Industry Standard, The , December 11, 2000 , v3 n50 p158-159, 2 Page(s)
ISSN: 1098-9196
Languages: English
Document Type: Articles, News & Columns
Geographic Location: United States
Discusses Web businesses' approach to network security. Reports that Web businesses use servers that conduct transactions with authorized parties outside the company network. Says that hackers employ devious means to trick these Web servers into granting them permission to access back-end databases. Mentions that Web businesses need to shield their network with hardware or software **firewalls** , **virtual private networks** (**VPNs**), encryption, and antivirus products. Defines the following terms: audit trail; back doors; black-hat hacker; buffer overflow; certificate authorit cracker; cryptography; denial of service; digital signature; **firewall** ; hacking; intrusion detection; key; key escrow; letter bomb; logic bomb; password crackers; public key infrastructure (PKI); Secure **Socket** Layer (**SSL**); smurfing; spoof; **VPN** ; and worm. Includes two photos and a sidebar. (MEM)
Descriptors: Network Security; Security Measures; Electronic Commerce; Hackers; Public Key Infrastructure; **Firewalls** ; **Virtual Private Networks**

11/5/16 (Item 9 from file: 233)
DIALOG(R)File 233:Internet & Personal Comp. Abs.

00610598 00IW09-105
Keys to the privacy-enabled enterprise -- Building trust across computing environments requires a combination of firewalls , VPNs , SSL , **PKI, digital certificates**
Borck, James R
InfoWorld , September 11, 2000 , v22 n37 p58, 60, 2 Page(s)
ISSN: 0199-6649
Languages: English
Document Type: Articles, News & Columns
Geographic Location: United States
Discusses the information technology (IT) infrastructure components of a privacy-enabled enterprise. Explains the threat to sensitive corporate and customer information via online exposure calls for strong transactional security measures. States failure to undertake the development of a security plan to defend one's company against security threats will result in eroding customer trust, failed partner confidence, and lost revenue. Mentions proper protection over distributed computing environments necessitates the following: assurances for data and transaction integrity; confidentiality during and after transit; user authentication and authorization in resource availability; and a method of nonrepudiation to ensure responsibility for transaction. Discusses the use of hashing, encryption, public key infrastructure, digital certificates, certificate authorities, and **virtual private networks** . Includes a photo and a sidebar. (MEM)
Descriptors: Privacy; Security; Infrastructure; Information Technology; Public Key Infrastructure; Digital Certificates; **Virtual Private Networks**

11/5/17 (Item 10 from file: 233)
DIALOG(R)File 233:Internet & Personal Comp. Abs.

00547019 99SR09-008
First Look; CRYPTOAdmin V4.0; PowerCrypt; CeloCom Kit
SC/Info Security News Magazine , September 1, 1999 , v10 n9 p24, 1 Page(s)
ISSN: 1096-7974
Company Name: CRYPTOCard; Global Technologies Group; Celo Communications
URL: http://www.cryptocard.com http://www.powercrypt.com http://www.celocom.com
Product Name: CRYPTOAdmin 4.0; PowerCrypt; CeloCom Kit
Languages: English
Document Type: Articles, News & Columns
Geographic Location: United States
Previews security products: CRYPTOAdmin V4.0 ($5,000) from CRYPTOCard (416); PowerCrypt ($NA) from Global Technologies Group (703); and CeloCom Kit ($NA) from Celo Communications (650). Calls CRYPTOAdmin a compatible environment for products like Steel-Belted RADIUS, Gauntlet **Firewall** , and CiscoSecure ACE, among others. Says as a client-server, it provides the type of token management a company needs, while integrating with other products that already support the CRYPTOCard. Notes PowerCrypt is hardware that enables a faster resource for the management of network security operations. Says the PCI card manages its own processor encryption functions and uses the HiFn 7751 encryption chip. Reports the CelCom Kit is three boxed products that work together for secure authentication, it enables encryption through TCP protocols using the **SSL tunnel** , and adds another layer of security to e-business transactions. Includes three photos. (sps)
Descriptors: Administration; Security; Encryption; Privacy; Secure Electronic Transaction; Electronic Commerce
Identifiers: CRYPTOAdmin 4.0; PowerCrypt; CeloCom Kit; CRYPTOCard; Global Technologies Group; Celo Communications

11/5/18 (Item 11 from file: 233)
DIALOG(R)File 233:Internet & Personal Comp. Abs.

00546390 99NC09-011
Securing POP and IMAP sessions -- E-mail security is nearly nonexistent. But there is promising work under way with challenge/response protocols
Backman, Dan
Network Computing , September 6, 1999 , v10 n18 p128-132, 3 Page(s)
ISSN: 1046-4468
Languages: English
Document Type: Articles, News & Columns
Geographic Location: United States
Discusses Post Office Protocol 3 (POP3) and Internet Messaging Access Protocol 4 (IMAP) electronic mail security on the network. Explains that POP3 and IMAP4 default to plain-text authentication. Suggests using transport-level encryption such as Internet Protocol Security (IPSec) or other **virtual private network** (**VPN**) technologies. Reports that vendors recognize the problem - that most attacks originate inside the **firewall** . Adds that they also realize the necessity of guarding users' passwords. Presents various non-clear-text POP and IMAP authentication solutions. Mentions that Microsoft Corp. and Netscape Communications Corp. provide client support for **SSL** POP and IMAP. Describes Qualcomm's implementation of Authentication POP (APOP) and Kerberos POP (KPOP). Discusses the Simple Authentication Security Layer (SASL) scheme. Includes one diagram and one photo. (MEM)
Descriptors: Electronic Mail; Security; Messaging; Internet Protocols ; Network Management; Networks

11/5/19 (Item 12 from file: 233)

DIALOG(R)File 233:Internet & Personal Comp. Abs.

00510116 98PK10-004
Sun acquires i-Planet to boost thin clients -- Startup's apps secure remote Web access, facilitate e-com
Surkan, Michael
PC Week , October 5, 1998 , v15 n40 p8, 1 Page(s)
ISSN: 0740-1604
Company Name: Sun Microsystems; i-Planet
Languages: English
Document Type: Articles, News & Columns
Geographic Location: United States
Focuses on the Java software of i-Planet Inc., which Sun Microsystems Inc. is about to acquire, and which will give Sun the technology to make thin clients more attractive alternatives to PCs. Explains that the as-yet-unnamed software takes Java applications and HTML and **tunnels** them securely through **firewalls** in Secure **Sockets** Layer (**SSL**)-encrypted sessions. Suggests that this could obviate the need for **virtual private networks** , because Web browsers have encrypted **SSL** , as well as the need for the heavy-client baggage normally required for remote access. Adds that this capability will also allow business-to-business e-commerce with a company's partners and suppliers, which will be able to securely access data from the company's network, such as the status of orders, without having to invest in expensive extranets. Includes one screen display.
Descriptors: Java; Mergers/Acquisitions; Diskless Workstation; Network Computer; **Firewalls** ; Encryption; Electronic Commerce
Identifiers: Sun Microsystems; i-Planet

11/5/20 (Item 13 from file: 233)
DIALOG(R)File 233:Internet & Personal Comp. Abs.

00508084 98JX09-004
Electronic commerce security
Cullinane, David
Journal of Information Systems Security , September 1, 1998 , v7 n3 p54-65, 12 Page(s)
ISSN: 1065-898X
Languages: English
Document Type: Articles, News & Columns
Geographic Location: United States
Focuses on electronic commerce security issues, noting that in two more years, there will be 500 million potential customers on the Internet needing only a PC and browser to make purchases. Proposes a process for developing secure electronic commerce which involves assessing the risks, securing the infrastructure, establishing secure Internet connections, conducting electronic commerce securely, and disaster recovery. Attention is given to information security architecture and policy, noting that one should develop an information security standard (SS), a network SS, external access SS, emergency response process, Internet security policy, **firewall** SS, and Web server SS. Also considers security tools and auditing, virus protection, scanning software, symmetric and asymmetric key encryption, encrypted **tunneling** , Secure **Sockets** Layer, Secure HTTP, hardware encryption, and the Secure Electronic Transaction Protocol. Includes one diagram and a list of resources. (jo)
Descriptors: Electronic Commerce; Security; Electronic Shopping; Internet; Information Management; Disaster Recovery; Standards

11/5/21 (Item 14 from file: 233)
DIALOG(R)File 233:Internet & Personal Comp. Abs.

00463324 97PK06-125
All network roads lead to VPNs : The sum of Mobile VPN 's parts doesn't add up to capabilities that are available elsewhere

Wold, Ken
PC WEEK , June 9, 1997 , v14 n23 p115-120, 2 Page(s)
ISSN: 0740-1604
Company Name: Aventail
Product Name: Mobile **VPN**
Languages: English
Document Type: Software Review
Grade (of Product Reviewed): B
Hardware/Software Compatibility: IBM PC Compatible; Microsoft Windows NT
Geographic Location: United States
Presents a favorable review of Mobile **VPN** ($4,995 for one server and 20 connections), a **virtual private network** (**VPN**) solution from Aventail Corp. of Seattle, WA (206). Runs on IBM PC compatibles with Windows NT. Explains that Mobile **VPN** is a proxy server which is targeted mainly as a remote access **VPN** solution, and also acts as a **firewall** to a limited degree, providing a secure data proxy channel through the Internet. Reports that Mobile **VPN** is easy to set up, configure, and use. Notes that it supports TCP, the Challenge Handshake Authorization Protocol, Secure **Sockets** Layer 3.0, DES, Triple DES, and RC4 for encryption. Notes that Mobile **VPN** is the first product to utilize SOCKSv5 technology. However, states that there are many **firewalls** that implement **VPN** solutions for nearly Mobile's price. Rates Mobile **VPN** a score of A for usability and manageability. Includes one screen display and a product summary. (jo)
Descriptors: Network Management; Server; Security; Cryptology; Networks; **Firewalls**
Identifiers: Mobile **VPN** ; Aventail

11/5/22 (Item 15 from file: 233)
DIALOG(R)File 233:Internet & Personal Comp. Abs.

00450543 97PQ02-095
Windows NT firewalls **are born**
Witt, Jeffrey G
PC Magazine-Network Edition , February 4, 1997 , v16 n3 pNE19-NE22, 3 Page(s)
ISSN: 0888-8507
Company Name: Global Internet; CheckPoint Software Technologies; Raptor Systems; NetGuard
Product Name: Centri **Firewall** 3.1; CheckPoint **FireWall** -1 for Windows NT 3.51, 2.1; Eagle NT 3.06; Guardian 2.0
Languages: English
Document Type: Buyer and Vendor Guide
Grade (of Product Reviewed): B; B; B; B
Hardware/Software Compatibility: Microsoft Windows NT
Geographic Location: United States
Presents a buyers' guide to Windows NT **Firewalls** . Features a table comparing price, recommended hardware, domain users and attributes, architecture, **VPN** , encryption, URL access control, and **SSL** support. Reviewed were: Centri **Firewall** 3.1 ($5,000 for 50 users) from Global Internet Inc. of Palo Alto, CA (800); CheckPoint **FireWall** -1 for Windows NT 3.51, 2.1 ($4,495 for 50 users) from CheckPoint Software Technologies Inc. of Redwood City, CA (800, 415); Eagle NT 3.06 ($6,500 for 50 users) from Raptor Systems Inc. of Waltham, MA (800); and Guardian 2.0 ($3,980 for 50 users) from NetGuard Inc. of Carrolton, TX (214). (phi)
Descriptors: **Firewalls** ; Software Review; Vendor Guide; Window Software; Security
Identifiers: Centri **Firewall** 3.1; CheckPoint **FireWall** -1 for Windows NT 3.51, 2.1; Eagle NT 3.06; Guardian 2.0; Global Internet; CheckPoint Software Technologies; Raptor Systems; NetGuard

11/5/23 (Item 16 from file: 233)
DIALOG(R)File 233:Internet & Personal Comp. Abs.

00435939 96PK09-413
Firewall **protects, serves -- All-in-one** Firewall **Server 4.0 provides gamut of simple Net tools**
Peterson, Eric
PC WEEK , September 30, 1996 , v13 n39 pN1, N9, 2 Page(s)
ISSN: 0740-1604
Company Name: Secure Computing
Product Name: BorderWare **Firewall** Server
Languages: English
Document Type: Software Review
Grade (of Product Reviewed): B
Geographic Location: United States
Presents a favorable review of BorderWare **Firewall** Server v4.0 ($7,000 for an unlimited-user license), an Internet connectivity package from Secure Computing Corp. of Roseville, MN (800). Comes with such standard Internet application tools as name, mail, FTP, news, and World Wide Web servers, along with optional support for **virtual private networks** (**VPNs**) and secure server networks. Notes that BorderWare implements the Internet Engineering Task Force's new IPsec digital encryption standard, and calls this the first product to support IPsec-based **VPNs** . States that you can use Netscape's Navigator 2.02 Web browser as BorderWare's administrative front end, which makes client setup much easier. However, complains that BorderWare's built-in Web server does not support CGI or **SSL** . Concludes that BorderWare can help small to medium-sized companies quickly establish secure Internet connectivity. Includes one screen display and a corporate buyers' advisory. (jo)
Descriptors: **Firewalls** ; Internet; Software Review; Security; Networks; Server
Identifiers: BorderWare **Firewall** Server; Secure Computing

11/5/24 (Item 17 from file: 233)
DIALOG(R)File 233:Internet & Personal Comp. Abs.

00435442 96PK09-011
FTP Software's OnNet32 2.0 easily provides the journeyman's tool kit
Phillips, Ken
PC WEEK , September 2, 1996 , v13 n35 pN7, N9, 2 Page(s)
ISSN: 0740-1604
Company Name: FTP Software
Product Name: OnNet32
Languages: English
Document Type: Software Review
Grade (of Product Reviewed): B
Hardware/Software Compatibility: IBM PC Compatible; Microsoft Windows 95; Microsoft Windows NT
Geographic Location: United States
Presents a favorable beta review of OnNet32 v2.0 ($NA), a TCP/IP protocol stack from FTP Software Inc. Runs on IBM PC compatibles with Windows 95 or Windows NT 4.0. Indicates that OnNet32 offers tight Windows 95 integration, strong security, and support for various protocols, as well as helpful wizards. Regarding Win95 integration, reports that OnNet32's configuration windows appeared in the Windows 95 Network Neighborhood Properties, and the FTP client imitated the Explorer interface. Features include support for IPv6, **Winsock** 2.0, and Mobile IP specifications; and support for Pretty Good Privacy for e-mail encryption and authentication, Secure **Sockets** Layer for financial transactions on the Web, NT domain security, **firewalls** , and **virtual private networks** . Also notes that OnNet32 provides workflow automation, and it is simple to set up. Says OnNet32 may have too many options for computer novices. Includes one screen display. (jo)
Descriptors: Network Management; Administration; Networks; Window Software; Software Review; Security
Identifiers: OnNet32; FTP Software

11/5/25 (Item 1 from file: 94)
DIALOG(R)File 94:JICST-EPlus

03906076 JICST ACCESSION NUMBER: 99A0155722 FILE SEGMENT: JICST-E
TCP/IP Tunneling **using** SSL .
KATAGIRI HIRONOBU (1); MARUYAMA HIROSHI (2)
(1) Tokyo Inst. of Technol. Fac. of Eng.; (2) IBM Japan Ltd., Tokyo Res. Lab. Comp. Sci. Inst.
Joho Shori Gakkai Shinpojiumu Ronbunshu, 1998, VOL.98,NO.12, PAGE.219-224, FIG.1, REF.6
JOURNAL NUMBER: Y0978BAT
UNIVERSAL DECIMAL CLASSIFICATION: 621.391.037.3 681.3:654
LANGUAGE: Japanese COUNTRY OF PUBLICATION: Japan
DOCUMENT TYPE: Conference Proceeding
ARTICLE TYPE: Original paper
MEDIA TYPE: Printed Publication
ABSTRACT: To access intranet applications securely from the Internet, a technique called **tunneling** or forwarding is known to be used. In this paper, we present a Java implementation of secure **tunneling** for forwarding any TCP/IP connections between a client outside a **firewall** and an internet server using Secure **Socket** Layer(**SSL**) as the transport protocol. Since the user authentication is based on X.509 digital certificate, secure and flexible trust hierarchy can be realized which greatly decreases the complexity of key management. (author abst.)
DESCRIPTORS: cryptography key; data protection; computer security; internet ; protocol; WWW(communication); authentication; information retrieval
BROADER DESCRIPTORS: cryptogram; protection; security; guarantee; computer network; communication network; information network; network; rule; information system; computer application system; system; retrieval
CLASSIFICATION CODE(S): ND02030R; JC03000K

11/5/26 (Item 1 from file: 111)
DIALOG(R)File 111:TGG Natl.Newspaper Index(SM)

07121633 Supplier Number: 75240413
Galea Secured Networks Chooses SSH IPSEC Express To Protect VPN , SSL **and** Firewall **Servers.**
Business Wire, 2082
June 4, 2001
LANGUAGE: English RECORD TYPE: Citation

FILE SEGMENT: NW File 649

11/5/27 (Item 1 from file: 6)
DIALOG(R)File 6:NTIS

0539549 NTIS Accession Number: N76-13180/4/XAB
An Investigation in Msfc 14-Inch Twt to Determine the Static Stability Characteristics of 0.004-Scale Model (74-Ots) Space Shuttle Vehicle 5 Configuration (IA33), Volume 1
(Aerothermodynamic Data Report)
Allen, E. C.
Chrysler Corp., New Orleans, La. Space Div.
Report No.: NASA-CR-141811; DMS-DR-2174-V-1
Oct 75 845p
Journal Announcement: GRAI7608; STAR1404
Seri-3.
Order this product from NTIS by: phone at 1-800-553-NTIS (U.S. customers); (703)605-6000 (other countries); fax at (703)321-8547; and email at orders@ntis.fedworld.gov. NTIS is located at 5285 Port Royal Road, Springfield, VA, 22161, USA.
NTIS Prices: PC A99/MF A01

Contract No.: NAS9-13247

Wind **tunnel** tests were conducted to: (1) determine the static stability characteristics of the Shuttle Vehicle 5 configuration; (2) determine the effect on the Vehicle 5 aerodynamic characteristics of External Tank (ET) and Solid Rocket Booster (SRB) nose shape, SRB nozzle shroud flare angle, orbiter to tank fairing, and sting location; (3) provide flow visualization using thin film oil paint; and (4) determine rudder, body flap, and inboard and outboard elevon hinge moments. The mated vehicle model was mounted in three different ways: (1) the orbiter mounted on the balance with the SRB's attached to the tank and the tank in turn attached to the orbiter; (2) the tank mounted on the balance (with the sting protruding through the tank base) with the SRB's and orbiter attached to the tank, and (3) with the tank mounted on the balance and the balance in turn supported by a forked sting entering the nozzle of each SRB, extending forward into the SRB's then crossing over to the tank to provide a balance **socket** . Data were obtained for Mach numbers from 0.6 through 4.96 at angles-of-attack and -sideslip from -10 to 10 degrees. (Author)

Descriptors: Scale models; *Space shuttle orbiters; *Static stability; *Wind **tunnel** stability tests; Aerodynamic characteristics; Aerodynamic **configurations** ; Elevons; Flow visualization; Rudders; Tables (**Data**); Wind **tunnel** models

Identifiers: NTISNASA

Section Headings: 84C (Space Technology--Manned Spacecraft)

11/5/28 (Item 1 from file: 99)

1733718 H.W. WILSON RECORD NUMBER: BAST98032314

How do I ensure secure communications from a Java applet?

Golomb, Kenneth; Sorgie, Thomas

Dr. Dobb's Journal v. 23 no6 (June '98) p. 107-9+
DOCUMENT TYPE: Feature Article ISSN: 1044-789X LANGUAGE: English
RECORD STATUS: Corrected or revised record

ABSTRACT: Ensuring secure communications from a Java applet by using HTTPS **tunneling** is discussed. **Data** is **tunneled** over the HTTPS protocol by wrapping it in another protocol stream. The Java applet client, the proxying service, and the application server must be considered in the **tunneling** process. **Tunneling** over HTTPS improves the performance and decreases the size of code, when compared with a Java implementation of the secure **sockets** layer.

DESCRIPTORS: Client server computing--Access control; Java applets;

15/5/1 (Item 1 from file: 238)
DIALOG(R)File 238:Abs. in New Tech & Eng.

0351333 ANTE NUMBER: 115197
Is your firewall **enough?**
AUTHOR(S): Oxley, P.
JOURNAL: Storage Handling Distribution 45 (6) Jun 2001 p.47, 49.
PUBLICATION YEAR: 2001
ISSN: 0039-1832
BLDSC SHELF MARK: 8466.360
LANGUAGE: English

ABSTRACT: Although a **firewall** is absolutely essential as a tool for guaranteeing the security of a company, a lot of work needs to be done at the planning stage to ensure that the correct **firewall security configuration** is chosen. In addition to, yet complimentary to, the **firewall** , consideration needs to be taken regarding: **virtual private networks** (**VPNs**); ServerLocking; intrusion detection; and monitoring, management and analysis. It is concluded that any company serious about network security needs to take a much broader approach that recognizes the crucial importance of information and the absolute necessity of protecting it; and one that truly integrates security throughout the business and matches the appropriate tools with the appropriate risks and involves staff in the security process.
DESCRIPTORS: Computers; Networks; Security systems; **Firewalls** ;

15/5/2 (Item 1 from file: 8)
DIALOG(R)File 8:Ei Compendex(R)

05232670 E.I. No: EIP99024571188
Title: Packet filtering in high speed networks
Author: Suri, Subhash; Varghese, George
Corporate Source: Washington Univ, St. Louis, MO, USA
Conference Title: Proceedings of the 1999 10th Annual ACM-SIAM Symposium on Discrete Algorithms
Conference Location: Baltimore, MD, USA Conference Date: 19990117-19990119
Sponsor: ACM
E.I. Conference No.: 49812
Source: Proceedings of the Annual ACM-SIAM Symposium on Discrete Algorithms 1999. SIAM, Philadelphia, PA, USA. p S969-S970
Publication Year: 1999
CODEN: PAAAF2
Language: English
Document Type: CA; (Conference Article) Treatment: G; (General Review); T; (Theoretical)
Journal Announcement: 9904W2
Abstract: The commercial viability of the future Internet depends on its ability to provide differentiated service to paying customers. The existing Internet delivers only the best effort service. Examples of differentiated service include **firewalls** for enterprise traffic sensitive routing. These services require Internet routers to move from simple destination-based packet forwarding to a more complex form of forwarding called layer 4 switching. In layer 4 switching, each router maintains a database of packet filters, each specifying values for some key header fields. The most common fields are the IP destination address, the IP source address, the protocol type, and the **port numbers** . Each field is specified as a variable length prefix. 6 Refs.
Descriptors: *Packet networks; Packet switching; Internet; Data communication systems; Network protocols; Telecommunication links; Telecommunication traffic; Telecommunication services; Data structures; Algorithms
Identifiers: Packet filtering; High speed networks; Point location algorithm; **Virtual private networks** (**VPN**); Naive filter matching algorithm

Classification Codes:
721.1 (Computer Theory, Includes Formal Logic, Automata Theory, Switching Theory, Programming Theory); 723.2 (Data Processing); 716.1 (Information & Communication Theory)
721 (Computer Circuits & Logic Elements); 716 (Radar, Radio & TV Electronic Equipment); 723 (Computer Software); 921 (Applied Mathematics)
72 (COMPUTERS & DATA PROCESSING); 71 (ELECTRONICS & COMMUNICATIONS); 92 (ENGINEERING MATHEMATICS)

15/5/3 (Item 2 from file: 8)
DIALOG(R)File 8:Ei Compendex(R)

04375991 E.I. No: EIP96043122686
Title: Internet and beyond: security data across the enterprise
Author: Pensak, David; Grandinetti, Mike
Source: International Journal of Network Management v 5 n 6 Nov-Dec 1995. p 305-312
Publication Year: 1995
CODEN: INMTEU ISSN: 1055-7148
Language: English
Document Type: JA; (Journal Article) Treatment: G; (General Review)
Journal Announcement: 9605W5
Abstract: Raptor System Inc., has developed a new model called 'the Five Domains of Network Security' to help administrators tackle the challenges of internetworking. The new model provides a roadmap for network managers to provide comprehensive protection across their entire information infrastructure. Domains 2 to 4 address security the most vulnerable elements within the enterprise including, the Internet, workgroup LANs, mobile personal computers, and remote sites. Domain 5 ties all these elements together, hence providing a central **security** envelope to **configure** , monitor and manage the enterprise-wide security solution from as many or as few sites as deemed necessary by the network manager.
Descriptors: *Computer networks; Security of data; Data communication systems; Local area networks; Personal computers; Network protocols; Information technology; Computer software; Data transfer; User interfaces
Identifiers: Business communication tools; Internet; Network security; Application level **firewalls** ; Information infrastructure; **Virtual private networks**
Classification Codes:
722.3 (Data Communication, Equipment & Techniques); 723.2 (Data Processing); 722.4 (Digital Computers & Systems); 723.5 (Computer Applications)
722 (Computer Hardware); 723 (Computer Software); 903 (Information Science)
72 (COMPUTERS & DATA PROCESSING); 90 (GENERAL ENGINEERING)

15/5/4 (Item 1 from file: 2)
DIALOG(R)File 2:INSPEC

7022930 INSPEC Abstract Number: B2001-10-7930-031, C2001-10-7150-003
Title: An information assurance architecture for army installations
Author(s): Hendy, T.; Troester, D.
Author Affiliation: US Army Inf. Syst. Eng. Command, Fort Huachuca, AZ, USA
Conference Title: MILCOM 2000 Proceedings. 21st Century Military Communications. Architectures and Technologies for Information Superiority (Cat. No.00CH37155) Part vol.1 p.444-8 vol.1
Publisher: IEEE, Piscataway, NJ, USA
Publication Date: 2000 Country of Publication: USA 2 vol. xxvii+1238 pp.
ISBN: 0 7803 6521 6 Material Identity Number: XX-2000-02174
U.S. Copyright Clearance Center Code: 0 7803 6521 6/2000/$10.00
Conference Title: Proceedings of IEEE Military Communications Conference (MILCOM'00)

Conference Sponsor: IEEE Commun. Soc.; Armed Forces Commun. & Electron. Assoc. (AFCEA)
Conference Date: 22-25 Oct. 2000 Conference Location: Los Angeles, CA, USA
Language: English Document Type: Conference Paper (PA)
Treatment: Applications (A); Practical (P)
Abstract: The increasing dependence information systems as the core Warfighter assets has prompted the US Army to make protecting its infrastructure of information systems and computer networks from attacks and disruption a top priority. This paper traces the development of an information assurance (IA) architecture for Army installations. Early in 1999, as a critical initiative within the Army's Installation Information Infrastructure Architecture (I3A) project, the Army's ODISC4 Architectures Directorate undertook the task of developing an IA architecture overlay that could be applied to Army installation communications and computer network backbones. Following DoD's Defense-In-Depth philosophy and taking into account current and emerging DoD and Army IA policies, a multiorganizational team continues to develop a flexible, capabilities-based IA architecture that blends Army IA concepts with accepted best practices from the commercial world. The emerging architecture is being applied to both ATM and TCP/IP networks and is enabling the Army to tailor installation IA implementations to meet unique mission requirements. The paper describes and discusses the various policies, capabilities, techniques, and types of produces that are currently included in the architecture including **firewalls** , security enabled routers, and proxy servers. Some of the challenges that are facing Army networks such as electronic commerce and issues associated with malicious code are presented along with potential solutions that are currently being investigated including the use of technologies like e-mail scanning servers and **virtual private networks** . Key efforts and initiatives undertaken by the 13A **Configuration** Control Board's **Information** Assurance Working Group to develop the concepts, policies, and management processes that the Army will need to maintain its IA enabled networks are also included. (0 Refs)
Subfile: B C
Descriptors: asynchronous transfer mode; computer network management; electronic commerce; information networks; Internet; military communication ; military computing; network servers; packet switching; security of data; telecommunication security; transport protocols
Identifiers: information assurance architecture; army installations; US Army; information systems protection; computer networks protection; network attacks; network disruption; Installation Information Infrastructure Architecture; ODISC4 Architectures Directorate; DoD; ATM networks; TCP/IP networks; **firewalls** ; security enabled routers; proxy servers; electronic commerce; malicious code; e-mail scanning servers; **virtual private networks** ; network management; Internet; network security
Class Codes: B7930 (Military communications); B6210L (Computer communications); B6210C (Network management); B6150M (Protocols); C7150 (Military computing); C5620W (Other computer networks); C7210N (Information networks); C6130S (Data security); C5640 (Protocols); C5630 (Networking equipment)

15/5/5 (Item 2 from file: 2)
DIALOG(R)File 2:INSPEC

6876715 INSPEC Abstract Number: B2001-05-6210L-013, C2001-05-6130S-004
Title: Getting personal with firewalls
Author(s): Dalton, C.E.
Journal: Network Magazine vol.16, no.1 p.100-2, 104, 106
Publisher: Miller Freeman,
Publication Date: Jan. 2001 Country of Publication: USA
CODEN: LANNER ISSN: 1093-8001
SICI: 1093-8001(200101)16:1L.100:GPWF;1-#
Material Identity Number: H420-2001-001
Language: English Document Type: Journal Paper (JP)

Treatment: General, Review (G)
Abstract: A personal **firewall** is designed to protect a single PC from undesired perusal and attack while connected to the Internet. **Firewalls** do this by inspecting both inbound and outbound traffic. **Firewalls** let the desired applications talk, while restricting all undesired or unknown data traffic, by using security policies the user defines. In a corporate scenario, a central policy server enforces a standard **security configuration** on the **firewalls** . Personal **firewalls** also need to handle intrusion detection, which entails notifying the user of the nature and source of an attack in progress. While secondary to prevention, intrusion detection can warn you of attacks that your current **firewall** security policy might not protect you from. **Firewalls** should be able to communicate securely with other hosts when required. While still uncommon in the personal **firewall** space, **VPN** technology is useful for this purpose. (0 Refs)
Subfile: B C
Descriptors: authorisation; business communication; Internet; microcomputers; telecommunication traffic
Identifiers: personal **firewall** ; PC; Internet; inbound traffic; outbound traffic; data traffic; security policies; corporate communication; central policy server; intrusion detection; **VPN** technology
Class Codes: B6210L (Computer communications); C6130S (Data security); C5620W (Other computer networks)

15/5/6 (Item 3 from file: 2)
DIALOG(R)File 2:INSPEC

5962699 INSPEC Abstract Number: B9808-6210L-108, C9808-5620W-027
Title: Secure Web tunneling
Author(s): Abadi, M.; Birrell, A.; Stata, R.; Wobber, E.
Author Affiliation: Syst. Res. Center, Digital Equip. Corp., Palo Alto, CA, USA
Journal: Computer Networks and ISDN Systems Conference Title: Comput. Netw. ISDN Syst. (Netherlands) vol.30, no.1-7 p.531-9
Publisher: Elsevier,
Publication Date: April 1998 Country of Publication: Netherlands
CODEN: CNISE9 ISSN: 0169-7552
SICI: 0169-7552(199804)30:1/7L.531:ST;1-M
Material Identity Number: I876-98002
U.S. Copyright Clearance Center Code: 0169-7552/98/$19.00
Conference Title: 7th International World Wide Web Conference
Conference Date: 14-18 April 1998 Conference Location: Brisbane, Qld., Australia
Document Number: S0169-7552(98)00048-8
Language: English Document Type: Conference Paper (PA); Journal Paper (JP)
Treatment: Practical (P)
Abstract: The boundary of an organization does not always coincide with its **firewall** . A member of an organization that is outside the **firewall** may wish to access internal WWW services with the same ease and security that are common within the **firewall** . At the same time, the **firewall** should still be able to perform adequate access control, logging, and auditing. We describe a new technique for secure Web **tunneling** , which permits the desired outside access to internal Web services. We argue that this technique is preferable to alternatives such as special **firewall configurations** , IP **tunneling** , and reverse proxies. We describe an implementation of Web **tunneling** that relies mostly on common, off-the-shelf components. (12 Refs)
Subfile: B C
Descriptors: authorisation; Internet
Identifiers: **firewall** ; WWW services; Web **tunneling** ; security; access
Class Codes: B6210L (Computer communications); C5620W (Other computer networks); C6130S (Data security); C7210 (Information services and centres)

15/5/7 (Item 1 from file: 233)
DIALOG(R)File 233:Internet & Personal Comp. Abs.

00648938 01EW11-214
Zeroing in on security administration -- NetScreen's Global Pro apps ease configuration of firewall , VPN **devices**
Carlson, Caron
eWeek , November 19, 2001 , v18 n45 p30, 1 Page(s)
ISSN: 0740-1604
Company Name: NetScreen Technologies
Product Name: Global Pro 3.0; Global Pro Express
Languages: English
Document Type: Articles, News & Columns
Geographic Location: United States
Announces the release of NetScreen Technologies Inc.'s two management applications to simplify the configuration of its **firewall** and **virtual private network** (**VPN**) devices. Says NetScreen's Global Pro 3.0 and Global Pro Express make security application administration easier by allowing network managers to configure large numbers of devices from one computer. Explains that rather than making changes to network security device by device, a manager can set a policy for a group of security devices and **VPN** clients and rapidly respond to attacks. Notes that Global Pro 3.0 not only enables group policy **configuration** , but also provides monitoring of **security** events and reporting. Adds that it configures and monitors as many as 10,000 NetScreen security systems and appliances. Indicates that Global Pro Express is built for smaller installations of up to 100 security devices. Includes a table. (NAR)
Descriptors: **Firewalls** ; **Virtual Private Networks** ; **Securi ty Measu** res; Network Security; Network Management; Security Breaches
Identifiers: Global Pro 3.0; Global Pro Express; NetScreen Technologies

15/5/8 (Item 2 from file: 233)
DIALOG(R)File 233:Internet & Personal Comp. Abs.

00648829 01NR11-105
Check Point tools ease VPN **administration**
Greene, Tim
Network World , November 12, 2001 , v18 n46 p21-22, 2 Page(s)
ISSN: 0887-7661
Company Name: Check Point Software Technologies
URL: http://www.checkpoint.com http://www.checkpoint.com http://www.checkpoint.com
Product Name: One Click **VPN** ; One Click Extranet; One Click Certificate
Languages: English
Document Type: Articles, News & Columns
Geographic Location: United States
Reports that Check Point Software Technologies is adding management features to its **VPN** -1/ **Firewall** -1 software which would make it easier for customers to add and **configure** their Internet protocol (IP) **security virtual private network** (**VPN**) sites. Says that three new tools, known as One Click **VPN** , One Click Extranet, and One Click Certificate, automate procedures for expanding **VPNs** and adding remote users, which saves time and eliminates manual processes that invite human error. Explains that One Click **VPN** asks users to enter the IP address of a new site, and then configures the new gateway with the policies that have been set for the **VPN** and distributes information about the site to the **VPN** gateways at all the other sites. Includes a screen display and a photo. (EPE)
Descriptors: **Virtual Private Networks** ; Network Management; Internet Protocols; Remote Computing; Gateway; Network Security
Identifiers: One Click **VPN** ; One Click Extranet; One Click

Certificate; Check Point Software Technologies

15/5/9 (Item 3 from file: 233)
DIALOG(R)File 233:Internet & Personal Comp. Abs.

00636262 01NR07-208
Big firewall in a small package -- NetScreen-500 firewall / VPN appliance packs a price/performance punch
Snyder, Joel
Network World , July 16, 2001 , v18 n29 p36-37, 2 Page(s)
ISSN: 0887-7661
Company Name: NetScreen
URL: http://www.netscreen.com
Product Name: NetScreen-500
Languages: English
Document Type: Hardware Review
Grade (of Product Reviewed): B
Geographic Location: United States
Presents a favorable review of the NetScreen-500 ($25,000), a **firewall** and **virtual private network** (**VPN**) appliance from NetScreen (403). Says it has up to four Gigabit Ethernet or up to eight Fast Ethernet interfaces. Describes the bridge-mode feature, which gives it unparalleled flexibility, use of 802.1Q virtual local area network (VLAN) tagging to simulate up to 25 separately managed **firewalls** , excellent price/performance ratio, and site-to-site Internet Protocol **Security** implementation that is easy to **configure** . Mentions, however, that the Web-based graphical user interface (GUI) may be too simple for enterprise managers. Concludes that it is well-positioned as a mainstream enterprise-sized **firewall** for users that need more power than the NetScreen-100 can deliver. On a scale ranging from 1 to 5, received the rating of 4.15. Includes a photo, a table, a sidebar, and a product summary. (MEM)
Descriptors: **Firewalls** ; **Virtual Private Networks** ; **Networ k Securi** ty; Security Measures
Identifiers: NetScreen-500; NetScreen

15/5/10 (Item 4 from file: 233)
DIALOG(R)File 233:Internet & Personal Comp. Abs.

00630660 01IW05-003
SOHO VPNs bring secure connections to all -- Falling broadband access costs and decreasing hardware prices have caused CTOs to rethink company policy on virtual private...
Fielden, Tim
InfoWorld , May 7, 2001 , v23 n19 p60, 1 Page(s)
ISSN: 0199-6649
Company Name: Perle Systems
URL: http://www.perle.com
Product Name: Perle Systems IOLINK-520
Languages: English
Document Type: Hardware Review
Grade (of Product Reviewed): B
Geographic Location: United States
Discusses **virtual private networks** (**VPNs**) for the small office and home office (SOHO) market. Reports that the low-cost SOHO **VPNs** use private network **tunneling** and **data** encryption in the same way that enterprise-level **VPNs** do. Presents a favorable review of the Perle Systems IOLINK-520 ($1,495), a **VPN** device from Perle Systems (800). Highlights its comprehensive security features, use of STAC LZS data compression, ease of **VPN** setup and administration, and support for Password Authentication Protocol (PAP) and Challenge Handshake Authentication Protocol (CHAP). Mentions, however, that it is limited to 10/100 configuration. Concludes that it merits consideration by information technology managers looking to implement a SOHO **firewall** , **VPN** , or

frame-relay connection to a remote user's location. On a scale ranging from 1 to 5, received the rating of 4. Includes a sidebar, a photo, and a product summary. (MEM)
Descriptors: **Virtual Private Networks** ; Small Business; Home Office; Remote Computing; Network Security; Connectivity; Encryption
Identifiers: Perle Systems IOLINK-520; Perle Systems

15/5/11 (Item 5 from file: 233)
DIALOG(R)File 233:Internet & Personal Comp. Abs.

00621513 01IK02-221
App locks down servers
Yasin, Rutrell
InternetWeek , February 19, 2001 , n849 p16, 1 Page(s)
ISSN: 0746-8121
Company Name: WatchGuard Technologies
Product Name: WatchGuard ServerLock
Languages: English
Document Type: Articles, News & Columns
Geographic Location: United States
Discusses WatchGuard ServerLock server security software from **firewall** and **virtual private network** (**VPN**) products vendor WatchGuard Technologies. Reports that ServerLock locks down Microsoft Windows NT and Windows 2000 servers. Explains that ServerLock integrates into the kernel of the operating system to restrict write access to files. Mentions that ServerLock can block attempts to modify a system's registry, which is the repositor all hardware, software, and application **configuration data** . out that ServerLock is designed for the information technology (manager with basic security skills. Indicates that using ServerLoc network administrators can place servers in either operational or administrative mode with one button click. Cites ServerLock's kernel-based encryption method. Includes a screen display. (MEM)
Descriptors: Security Measures; Server; Network Server; Operating Systems; Client-Server Computing; Encryption
Identifiers: WatchGuard ServerLock; WatchGuard Technologies

15/5/12 (Item 6 from file: 233)
DIALOG(R)File 233:Internet & Personal Comp. Abs.

00616311 00IK12-114
Raley's goes shopping for cheaper access
Zimmerman, Christine
InternetWeek , December 11, 2000 , n841 p27, 1 Page(s)
ISSN: 0746-8121
Company Name: Raley's; Intel Corp.
Product Name: Express 8205 **VPN** Broadband Router
Languages: English
Document Type: Articles, News & Columns
Geographic Location: United States
Reports that retail chain Raley's is deploying the Express 8205 **VPN** Broadband Router from Intel Corp. Says that with the device, protected **virtual private network** (**VPN**) **tunnels** are established between the router and the **VPN** gateway, where traffic enters and exits the **VPN** . Mentions that the product offers security for ``always on'' connections in branch and small offices. Enumerates the router's features: autosensing 10/100 BaseT local area netw (LAN) port; Intel 960JT processor; Intel Device View management software; **firewall** event logging; Internet Protocol Security- (IPSec) **tunneling** with **Data** Encryption Standard (DES), Triples DE (3DES), and RC4 encryption; interoperability with third-party V solutions; and support of unlimited users. Includes a sidebar. (MEM)
Descriptors: **Virtual Private Networks** ; Router; Security; Internet Access; Enterprise Computing; Broadband Communication; Encryption

Identifiers: Express 8205 **VPN** Broadband Router; Raley's; Intel Corp.

15/5/13 (Item 7 from file: 233)
DIALOG(R)File 233:Internet & Personal Comp. Abs.

00614595 00NC11-106
Managing remote office connections -- Remote management is fraught with difficulties. Here's how to avoid losing touch
Fratto, Mike
Network Computing , November 13, 2000 , v11 n22 p168-174, 4 Page(s)
ISSN: 1046-4468
Languages: English
Document Type: Articles, News & Columns
Geographic Location: United States
Presents guidelines for network and systems managers on managing remote-office networks. Cites the first step to look at basic connectivity. Says that regardless of connection type or Internet service provider (ISP), having an in-bound dial backup for out-of-band management is crucial. Mentions the necessity of security measures at the remote site, comprising passwords, caller identification on telephones, encrypted modems, **firewall** , and **virtual private network** . Indicates that it does not make sense in many cases to purchase routable Internet addresses for each remote offices. Explains Network **Address Port** Translation (NAPT). Presents a remote-office-management checklist: out-of-band management, remote-manageme nt station, remote-control software, encryption software, good passwords, and technical support numbers. Includes a diagram and a table. (MEM)
Descriptors: Remote Computing; Network Management; Security Measures; Connectivity; Encryption; Enterprise Computing; Client-Server Computing

15/5/14 (Item 8 from file: 233)
DIALOG(R)File 233:Internet & Personal Comp. Abs.

00552383 99MW11-010
SonicWall Pro -- Speedy firewall **delivers 100 Mbps**
Beckman, Mel
Macworld , November 1, 1999 , v16 n11 p68, 1 Page(s)
ISSN: 0741-8647
Company Name: Sonic Systems
URL: http://www.sonicsys.com
Product Name: SonicWall Pro
Languages: English
Document Type: Hardware Review
Grade (of Product Reviewed): B
Hardware/Software Compatibility: Macintosh
Geographic Location: United States
Presents a favorable review of the SonicWall Pro Internet **firewall** device ($2,995) from Sonic Systems (888). Describes it as a dedicated, Web-administered network appliance for connecting private LANs to the Internet. Says that SonicWall Pro breaks the 10-Mbps barrier with three 100-Mbps Ethernet ports, a high-speed RISC processor, and a rack-mountable enclosure. Believes that it delivers the performance today's business LANs demand of their **firewalls** . Thinks that its **VPN** support and rack-ready packaging make it a great choice for high-speed **security** . Likes its Web-based **configuration** , **VPN** support, built-in DHCP server, and excellent performance. However, notes that it does not have Internet Key Exchange support and that it lacks Macintosh **VPN** client software. Rated four on a scale of one to five. Includes one photo. (CT)
Descriptors: **Firewalls** ; Local Area Networks; Internet; Security; Ethernet
Identifiers: SonicWall Pro; Sonic Systems

15/5/15 (Item 9 from file: 233)
DIALOG(R)File 233:Internet & Personal Comp. Abs.

00513581 98NC11-120
cIPro-DMZ: More VPN **for your dollar**
Fratto, Mike
Network Computing , November 15, 1998 , v9 n21 p30-32, 2 Page(s)
ISSN: 1046-4468
Company Name: RADGUARD
URL: http://www.radguard.com
Product Name: RADGUARD cIPro-DMZ
Languages: English
Document Type: Hardware Review
Geographic Location: United States
Presents a preview of the cIPro-DMZ **VPN** gateway consolidator ($8,950) from RADGUARD of NJ (201). Reports that its function is to consolidate two cIPro- **VPN** gateways into the same unit, but let the two **VPNs** handle traffic and management individually while sharing housing and power supplies. Explains that since the two **VPNs** operate separately, they require their own security, calling that fact a plus because performance degradation on any traffic segment managed by one **VPN** will not negatively impact traffic on the other. Indicates that the two **VPNs** can also be used in a configuration in which one of them performs all the management functions while the second operates as a **firewall** . Appreciates that it provides network managers with flexibility when **configuring** network **security** . Includes two flowcharts, one screen display, and one photo. (CAT)
Descriptors: Network Management; Networks; **Firewalls**
Identifiers: RADGUARD cIPro-DMZ; RADGUARD

15/5/16 (Item 10 from file: 233)
DIALOG(R)File 233:Internet & Personal Comp. Abs.

00511147 98PK10-311
Tall walls for small halls -- Sonic Systems' SonicWall has good feature set for small networks
Wold, Ken
PC Week , October 26, 1998 , v15 n43 p116, 1 Page(s)
ISSN: 0740-1604
Company Name: Sonic Solutions
URL: http://www.sonicsys.com
Product Name: SonicWall
Languages: English
Document Type: Software Review
Grade (of Product Reviewed): B
Hardware/Software Compatibility: IBM PC Compatible
Geographic Location: United States
Presents a favorable review of SonicWall ($495, 10 users and two NICS; $1,795, unlimited users and three NICs) from Sonic Systems Inc. of Sunnyvale, CA (800). Indicates that this Internet **firewall** is robust enough for home or branch offices' Internet **firewall** needs and offers tight security for small LANs. However, notes that its lack of scalability and fault tolerance will keep it out of larger enterprises' security plans. Points out that it lacks **virtual private network** (**VPN**) support, has no fault tolerance or centralized management, is not scalable, and needs **security configuration** wizards. Says that it comes with a Dynamic Host Configuration Protocol server to help ease the burden of internet protocol (IP) address assignment for the network administrator. Points out that it would perform well in small business environments, commenting there were no competing products in this class for this price. Includes one screen display and a product summary. (MAP)
Descriptors: **Firewalls** ; Security; Internet; Small Business; Local Area Networks
Identifiers: SonicWall; Sonic Solutions

15/5/17 (Item 11 from file: 233)

DIALOG(R)File 233:Internet & Personal Comp. Abs.

00507808 98PK09-007

Tapping browser power for collaboration -- ActiveMeetings beta eases conferencing, but some tools limited

Kramer, Matt

PC Week , September 7, 1998 , v15 n36 p51, 54, 2 Page(s)

ISSN: 0740-1604

Company Name: ActiveTouch

URL: http://www.activetouch.com

Product Name: ActiveMeetings

Languages: English

Document Type: Software Review

Grade (of Product Reviewed): B

Hardware/Software Compatibility: IBM PC Compatible; Microsoft Windows 95

Geographic Location: United States

Presents a favorable beta review of ActiveMeetings ($NA), a Web-based collaboration tool from ActiveTouch Inc. of Sunnyvale, CA (408). Runs on IBM PC compatibles with Windows 95. Explains that ActiveMeetings includes server-based collaboration tools that use Web browsers as clients, unlike competitors which require a separate client to implement the T.120 collaboration protocol. States that ActiveMeetings installs ActiveX control plug-ins to Web browsers, and uses a modified version of T.120 that employs HTTP **tunneling** to send meeting **data** , making it easier to communicate through **firewalls** that might block native T.120 traffic. Features include shared whiteboards, application sharing, and the ability to deliver presentations and annotate documents. Complains about its slow application sharing performance; however, notes that ActiveMeetings offers a quick, easy way to hold an online meeting. Includes one screen display and a product summary.

Descriptors: Collaboration; Workgroup Computing; Client-Server Computing; Web Browsers; ActiveX; Web Tools

Identifiers: ActiveMeetings; ActiveTouch

15/5/18 (Item 12 from file: 233)

DIALOG(R)File 233:Internet & Personal Comp. Abs.

00507552 98NC09-110

Network address translation: hiding on plain sight

Fratto, Mike

Network Computing , September 15, 1998 , v9 n17 p110-113, 3 Page(s)

ISSN: 1046-4468

Languages: English

Document Type: Articles, News & Columns

Geographic Location: United States

Presents an overview of Network Address Translation (NAT) as a means for resolving IP address conflicts. Explains that NAT devices work to map unregistered IP addresses to registered ones, using three different methods: static NAT, pooled NAT, and port-level NAT or **Port Address** Translation (PAT). Reports that all three methods performed successfully when tested, and notes that advantages of each depends on how it is to be used. Mentions that there are also security issues to be addressed when utilizing NAT, and suggests that an NAT device not be placed outside a **firewall** or on unprotected sides of a **VPN** . Concludes that NAT is a simple solution to IP addressing problems, although it requires administrators to take precaution against security problems. Includes two diagrams. (kgh)

Descriptors: Internet Protocols; Administration; Management; Network Management; **Firewalls** ; Virtual LANs; Security

15/5/19 (Item 13 from file: 233)

DIALOG(R)File 233:Internet & Personal Comp. Abs.

00496200 98SQ05-013
Guardian
, May 1, 1998 , v9 n5 p39, 1 Page(s)
Company Name: LanOptics
URL: http://www.NTFirewall.com
Product Name: Guardian 3.0
Document Type: Software Review
Grade (of Product Reviewed): A
Hardware/Software Compatibility: IBM PC Compatible; Microsoft Windows NT
Geographic Location: United States
Presents a very favorable review of Guardian 3.0 ($3,980), a **firewall** from LanOptics, Inc. (972). Runs on IBM PC compatibles with Windows NT. Explains that Guardian offers stateful inspection technology with a MAC-layer inspection engine providing high levels of security and performance. Reports that Guardian is easy to use, and a wizard steps the administrator through the installation and **configuration** process of creating the initial **security** policy Features include ODBC-compatible log databases; bandwidth control; **VPN** , NAT and user authentication; and the ability to monitor usage of the **firewall** in real-time, right down to individual user and session level. Rates Guardian five out of five stars overall; three stars for documentation; four stars for support and performance; and five stars for features, ease of use for novice or professional, and value for the money. Awards Guardian the SC Editor's Choice seal Includes one screen display and a product summary
Descriptors: **Firewalls** ; Security; Networks; Network Management; Administration
Identifiers: Guardian 3.0; LanOptics

15/5/20 (Item 14 from file: 233)
DIALOG(R)File 233:Internet & Personal Comp. Abs.

00481254 97IW12-309
Interpol's simple but secure firewall **box is ideal for small networks**
Hall, Eric
InfoWorld , December 22, 1997 , v19 n51/52 p48C, 1 Page(s)
ISSN: 0199-6649
Company Name: Sonic Systems
URL: http://www.sonicsys.com
Product Name: Sonic Interpol
Languages: English
Document Type: Hardware Review
Grade (of Product Reviewed): C
Geographic Location: United States
Presents a mixed review of Interpol ($1,999), an Internet **firewall** solution from Sonic Systems Inc. of Sunnyvale, CA (888). Explains that this is a self-contained solution featuring Ethernet ports for Internet router connection, private internal network, and external public network. Also features built-in browser-based configuration and management software plus a set of content filtering tools. Explains that it emulates an IP Ethernet bridge, responding to ARP requests for devices on each segment. Explains that it monitors the activity of any incoming packets, allowing temporary access only to those requested from inside. Complains that there is a limited **number** of TCP **ports** , and that there are no options for **virtual private network** services. Concludes that this is a good solution for smaller businesses, though its limited TCP ports make it a poor choice for larger enterprises. Rated three out of five. Includes one screen display and one product summary. (kgh)
Descriptors: Network Management; **Firewalls** ; Ethernet; Security; Software Tools; Virtual LANs
Identifiers: Sonic Interpol; Sonic Systems

15/5/21 (Item 15 from file: 233)
DIALOG(R)File 233:Internet & Personal Comp. Abs.

00472059 97DC09-102
VPNs : **security with an uncommon touch -- There's more than one way to manage secure links over the 'Net - but some are easier than others**
Shah, Deval; Holzbaur, Helen
Data Communications , September 21, 1997 , v26 n12 p52-63, 10 Page(s)
ISSN: 0363-6399
Company Name: Check Point Software Technologies; Sun Microsystems; Isolation Systems; Timestep
Product Name: **Firewall** 1 3.0; Sunscreen EFS 1.1; InfoCrypt Enterprise; Permit Security Gateway
Languages: English
Document Type: Buyer and Vendor Guide
Grade (of Product Reviewed): A; A; A; A
Hardware/Software Compatibility: IBM PC Compatible; Unix workstation; Microsoft Windows
Geographic Location: United States
Presents a buyers' guide to **virtual private network** products. Features a table comparing the topologies, integrated **firewall** , LAN ports, authentication, encryption, key management, **tunneling** , secure remote **configuration** , log-full handling, operating system, and price for a server and 100 connections of 14 products from 14 companies. Given Tester's Choice awards are **Firewall** 1 3.0 ($18,900) from Check Point Software Technologies Ltd. of Redwood City, CA, (415) which features ease of use; InfoCrpt Enterprise ($9,950) from Isolation Systems Ltd. of Toronto, ON, (416) which displays all devices and **VPN tunnels** ; Sunscreen EFS 1.1 ($4,995) from Sun Microsystems of Mountain View, CA, (512) which eases setting up a **VPN** ; and Permit Security Gateway ($32,850) from Timestep Corp. of Kanata, ON, (613) which simplifies the use of certificate authorities. Includes two photos, two screen displays, benchmark test results, a diagram, a chart, report card, and a resource guide. (dpm)
Descriptors: Networks; Internetworking; Software Tools; Server; **Firewalls** ; Digital Certificates
Identifiers: **Firewall** 1 3.0; Sunscreen EFS 1.1; InfoCrypt Enterprise ; Permit Security Gateway; Check Point Software Technologies; Sun Microsystems; Isolation Systems; Timestep

15/5/22 (Item 16 from file: 233)
DIALOG(R)File 233:Internet & Personal Comp. Abs.

00471635 97IW09-308
Isolation Systems' VPN **network toaster ready for prime time**
McClure, Stuart
InfoWorld , September 22, 1997 , v19 n38 p54C, 54F, 2 Page(s)
ISSN: 0199-6649
Company Name: Isolation Systems
Product Name: InfoCrypt Enterprise 2.96p
Languages: English
Document Type: Hardware Review
Grade (of Product Reviewed): B
Hardware/Software Compatibility: IBM PC Compatible; Microsoft Windows NT; Microsoft Windows 95
Geographic Location: United States
Presents a favorable review of InfoCrypt Enterprise 2.96p ($5,400), a multifunction **virtual private network** device from Isolation Systems Ltd. of Toronto, ON (888). Runs on Windows 95 and NT that is supported by InfoCrypt Manager software. Says that it offers an appliance-like **firewall** , routing, and **virtual private network** functions. Adds that it provides elegant configuration, certificate-based authentication, better-than-average encryption, and software updating. However, says that it has limited routing capabilities, is not IPSec-compliant, and has **firewall** proxies that require TCP/IP **port - number** knowledge. Concludes that ``a few limitations, this solution is a formidable offering in a crowded market niche.'' Rates four out of five points. Includes one screen

display, one diagram, and one report card. (dpm)
Descriptors: Virtual LANs; Networks; Network Management; **Firewalls** ; Cryptology; Router; Security
Identifiers: InfoCrypt Enterprise 2.96p; Isolation Systems

15/5/23 (Item 17 from file: 233)
DIALOG(R)File 233:Internet & Personal Comp. Abs.
(c) 2002 Info. Today Inc. All rts. reserv.

00462916 97CW06-409
Department firewalls **can hamper management**
Dryden, Patrick
Computerworld , June 30, 1997 , v31 n26 p49, 52, 2 Page(s)
ISSN: 0010-4841
Company Name: Hewlett-Packard; Dun & Bradstreet
Languages: English
Document Type: Articles, News & Columns
Geographic Location: United States
Discusses **firewalls** that guard the perimeter of an organization, but can also shut out information systems managers and external service providers who need to monitor networks and systems. Says that **firewalls** must be configured to allow passage of management traffic. Reports that Hewlett-Packard and Co.'s service organization has complained of not being able to monitor accounting and personnel departments protecting salary data. Explains that the IS group and the **security** department must **configure tunnels** or virtual connections between the central management station and the nodes to be managed. Highlights The Dun & Bradstreet Corp.'s internal **firewall** that separates systems accessed by customers from the corporate network. Adds that the **firewall** allows traffic betwee management console and targeted devices defined by specific IP addresses. Includes one sidebar. (smg)
Descriptors: **Firewalls** ; Network Management; Security; Corporate Strategy; Information Services; Networks; Case Study
Identifiers: Hewlett-Packard; Dun & Bradstreet

15/5/24 (Item 18 from file: 233)
DIALOG(R)File 233:Internet & Personal Comp. Abs.
(c) 2002 Info. Today Inc. All rts. reserv.

00432547 96WW08-124
Digging the IP tunnels **-- Net less expensive than private lines**
Booker, Ellis
WebWeek , August 19, 1996 , v2 n12 p37-38, 2 Page(s)
ISSN: 1081-3071
Languages: English
Document Type: Feature Articles and News
Geographic Location: United States
Discusses the potential of the Internet as a means of data transfer between private corporate networks. Explains that the **virtual private networks** (**VPN**) solution uses encryption and encapsulation to **tunnel data** through the Internet from one **firewall** -protected network to another. Notes that this is a much less expensive solution than private lines. Also points out that **VPNs** are much more flexible than leased lines, in that changes are much more easily implemented. Spotlights adoption of **VPNs** by TradeWave Corp. and Digital Equipment Corp., which claims that savings over private lines is up to 50 percent. Also mentions several **tunneling** products that have been made available. Indicates that some are unsure of service and security in the freeform environment of the public Internet. Includes one diagram. (kgh)
Descriptors: Internet; Networks; Data Transmission; Security; **Firewalls** ; Intranets

15/5/25 (Item 1 from file: 583)
DIALOG(R)File 583:Gale Group Globalbase(TM)
(c) 2002 The Gale Group. All rts. reserv.

06646817
WatchGuard Technologies reveals
WORLD: NEW FIREBOX II APPLIANCE FROM WATCHGUARD
Computerworld (XCK) 18 Jun 1998 P.11
Language: ENGLISH

The new Firebox II appliance has been launched by WatchGuard Technologies globally and targets businesses with branch offices/expanded networks. The US$ 4,995 Firebox II is a network-attachable **security** appliance which achieves remote network **configuration** and policy updates automation. The hardware and software appliance includes an IP Security-compliant **virtual private network** , **firewall** protection and encryption capabilities.

COMPANY: WATCHGUARD TECHNOLOGIES

PRODUCT: Computers & Auxiliary Equip (3573); Communications Eqp ex Tel (3662); Computer & Data Security Software (7372CD); Computer Services (7370); Intruder Prevention Systems (3662IP);
EVENT: Product Design & Development (33);
COUNTRY: General Worldwide (0W);

15/5/26 (Item 2 from file: 583)
DIALOG(R)File 583:Gale Group Globalbase(TM)

06305674
Digital Prepares To Introduce Software Family
US: DIGITAL TO LAUNCH ALTAVISTA SOFTWARE
Wall Street Journal Europe (WSJ) 07 May 1996 p.7
Language: ENGLISH

Indicating its increased commitment to the Internet and intranet markets, Digital Equipment of the US, is to introduce a range of AltaVista software. The software will buoy its AltaVista free Internet search service which is the Web's most-used search service. The software will come in Personal, Workgroup and Enterprise versions and will include features such as email, **tunnelling** (secure transfer of **data**) and **firewall** (data security) in addition to standard search. Many of the products will be rebranded Digital offerings as the company believes its own name is less well known on the Web than that of AltaVista.

COMPANY: DIGITAL EQUIPMENT; INTERNET

PRODUCT: Computers (3573CO); Computer Software (7372);
EVENT: Product Design & Development (33); Planning & Information (22);
COUNTRY: United Kingdom (4UK);

File 256:SoftBase:Reviews,Companies&Prods. 85-2002/Dec
(c)2002 Info.Sources Inc
File 278:Microcomputer Software Guide 2001/Dec
(c) 2001 Reed Elsevier Inc.

Set	Items	Description
S1	1532	FIREWALL? ? OR (BASTION OR PROXY)()HOST? ? OR APPLICATION(-)(GATEWAY? ? OR GUARD? ?)
S2	859	TUNNEL? OR VIRTUAL()PRIVATE()NETWORK? OR VPN OR VPNS
S3	19996	AUTHENTICAT? OR VERIF? OR VALIDAT? OR IDENTIF? OR SCREEN??? OR CHECK??? OR AUTHORIZ? OR AUTHORIS? OR PERMIT? OR PERMISSION
S4	825	SOCKET? ? OR WINSOCK OR SSL
S5	756	(CONFIGUR? OR TUNNEL?)(3N)(DATA OR INFORMATION) OR PORT? ?(3N)(NUMBER? OR ADDRESS? OR ID OR IDENTIF???? OR IDENTIFICATION) OR SESSION? ?(3N)(ID OR IDENTIF???? OR IDENTIFICATION OR DATA OR INFORMATION) OR (SECURITY OR TUNNEL?)(5N)CONFIGUR?
S6	1	S1 AND S2 AND S4 AND S5
S7	2	S2 AND S4 AND S5

7/5/1 (Item 1 from file: 256)
DIALOG(R)File 256:SoftBase:Reviews,Companies&Prods.

00115996 DOCUMENT TYPE: Review

PRODUCT NAMES: C50 (747947)

TITLE: No-Sweat setup for big VPNs
AUTHOR: Chowdhry, Pankaj
SOURCE: PC Week, v16 n15 p97(2) Apr 12, 1999
ISSN: 0740-1604

RECORD TYPE: Review
REVIEW TYPE: Review
GRADE: A

Altiga Networks' C50, a new **virtual private network** (**VPN**) concentrator, resolves the two most challenging problems blocking deployment of **VPNs** in large businesses: very difficult setup and little scalability. Two C50s, which are rated very good overall, were carefully tested for administration tools and for Triple Data Encryption Standard (DES) encryption performance. Triple DES performance was particularly good, with encrypted traffic throughput at 27Mbps using the 512-byte packet size generally sent over the Internet. This rate is the highest seen by testers. However, World Wide Web-based management needs improvement, since the internal Web server on the C50 is not Transport Layer **Security** -ready, and all **configuration** is done in the clear. The C50 can perform either as a LAN-to-LAN gateway or a client-to-LAN system. Ziff-Davis Benchmark Operation's Network Infrastructure Testing Tools was used to test client software, and allowed testers to work the **Winsock** layer of the client computers to determine their performance under actual network conditions. Configuring the C50 is easy, but requires extensive knowledge of **VPN** sites and their interfaces.

PRICE: $50000

COMPANY NAME: Cisco-Altiga Networks (661953)
SPECIAL FEATURE: Graphs Charts
DESCRIPTORS: Firewalls; Communications Interfaces; Network Administration Tools; Computer Security; Encryption; Internetworking; LANs; WANs; Intranets; Internet Security; System Monitoring
REVISION DATE: 20011029

7/5/2 (Item 2 from file: 256)
DIALOG(R)File 256:SoftBase:Reviews,Companies&Prods.

00099805 DOCUMENT TYPE: Review

PRODUCT NAMES: IP 6 (834092); IP 4 (834092)

TITLE: The Big IP Squeeze
AUTHOR: Kosiur, Dave
SOURCE: PC Week, v14 n4 p77(3) Jan 27, 1997
ISSN: 0740-1604

RECORD TYPE: Review
REVIEW TYPE: Product Analysis
GRADE: Product Analysis, No Rating

A thorough discussion of Internet Protocol 6 (IP 6), the new Internet protocol technology, shows how it will effect corporate intranets and Internet service providers, including a list of the steps necessary for the upgrade from IP 4. Benefits of IPv6 include vastly increased address space, more efficient routing, and easier management of assigning host addresses. Most notable is the increase in Net address space. IP 6's 128-bit address

field will allow for 60,000 trillion trillion addresses per person for the world population as of 1996. This is compared to the current IP 4's 32-bit field, providing for 4.3 billion addresses. With the increased space will come increased retooling of current systems, including loading stocks on every host, upgrading the software on the Domain Naming System (DNS) servers and routers, adding RAM to the routers, and manually **configuring tunnels** . On the up side, IPv6 technology should eliminate the tedious chore of assigning addresses to hosts. IP 6 is not backward compatible with IP 4. New technology called **tunneling** , however, should allow the two protocols to co-exist, smoothing the way for transition. Software for both hosts and routers is expected. Hewlett-Packard, Digital Equipment, and Sun Microsystems will add IP 6 to their UNIX operating systems, with **WinSock** 2.0 already offering support for it.

COMPANY NAME: Vendor Independent (999999)
SPECIAL FEATURE: Charts
DESCRIPTORS: Internetworking; Communications Protocols; Network Software; Communications Standards; Internet Utilities
REVISION DATE: 20010730

```
File 275:Gale Group Computer DB(TM) 1983-2002/Jan 29
         (c) 2002 The Gale Group
File 583:Gale Group Globalbase(TM) 1986-2002/Jan 28
         (c) 2002 The Gale Group
File  47:Gale Group Magazine DB(TM) 1959-2002/Jan 29
         (c) 2002 The Gale group
File 621:Gale Group New Prod.Annou.(R) 1985-2002/Jan 29
         (c) 2002 The Gale Group
File 636:Gale Group Newsletter DB(TM) 1987-2002/Jan 29
         (c) 2002 The Gale Group
File  16:Gale Group PROMT(R) 1990-2002/Jan 29
         (c) 2002 The Gale Group
File 160:Gale Group PROMT(R) 1972-1989
         (c) 1999 The Gale Group
File 148:Gale Group Trade & Industry DB 1976-2002/Jan 29
         (c)2002 The Gale Group
File 623:Business Week 1985-2002/Jan 28
         (c) 2002 The McGraw-Hill Companies Inc
File 624:McGraw-Hill Publications 1985-2002/Jan 29
         (c) 2002 McGraw-Hill Co. Inc
File  98:General Sci Abs/Full-Text 1984-2001/Dec
         (c) 2002 The HW Wilson Co.
File 553:Wilson Bus. Abs. FullText 1982-2001/Nov
         (c) 2001 The HW Wilson Co
File  88:Gale Group Business A.R.T.S. 1976-2002/Jan 29
         (c) 2002 The Gale Group
File  15:ABI/Inform(R) 1971-2002/Jan 29
         (c) 2002 ProQuest Info&Learning
File 635:Business Dateline(R) 1985-2002/Jan 29
         (c) 2002 ProQuest Info&Learning
File   9:Business & Industry(R) Jul/1994-2002/Jan 28
         (c) 2002 Resp. DB Svcs.
File 810:Business Wire 1986-1999/Feb 28
         (c) 1999 Business Wire
File 647:CMP  Computer Fulltext 1988-2002/Jan W3
         (c) 2002 CMP Media, LLC
File 674:Computer News Fulltext 1989-2002/Jan W2
         (c) 2002 IDG Communications
File 696:DIALOG Telecom. Newsletters 1995-2002/Jan 28
         (c) 2002 The Dialog Corp.
File 369:New Scientist 1994-2002/Jan W2
         (c) 2002 Reed Business Information Ltd.
File 813:PR Newswire 1987-1999/Apr 30
         (c) 1999 PR Newswire Association Inc
File 613:PR Newswire 1999-2002/Jan 29
         (c) 2002 PR Newswire Association Inc
File 634:San Jose Mercury  Jun 1985-2002/Jan 27
         (c) 2002 San Jose Mercury News
File 370:Science 1996-1999/Jul W3
         (c) 1999 AAAS

Set     Items   Description
S1     128820   FIREWALL? ? OR (BASTION OR PROXY)()HOST? ? OR APPLICATION(-
              )(GATEWAY? ? OR GUARD? ?)
S2     282630   TUNNEL? OR VIRTUAL()PRIVATE()NETWORK? OR VPN OR VPNS
S3    7255844   AUTHENTICAT? OR VERIF? OR VALIDAT? OR IDENTIF? OR SCREEN???
               OR CHECK??? OR AUTHORIZ? OR AUTHORIS? OR PERMIT? OR PERMISSI-
              ON
S4     122342   SOCKET? ? OR WINSOCK OR SSL
S5     102715   (CONFIGUR? OR TUNNEL?)(3N)(DATA OR INFORMATION) OR PORT? ?-
              (3N)(NUMBER? OR ADDRESS? OR ID OR IDENTIF???? OR IDENTIFICATI-
              ON) OR SESSION? ?(3N)(ID OR IDENTIF???? OR IDENTIFICATION OR -
              DATA OR INFORMATION) OR (SECURITY OR TUNNEL?)(5N)CONFIGUR?
S6         18   S1(S)S2(S)S3(S)S4(S)S5
S7         10   RD (unique items)
S8         32   S1(S)S2(S)S4(S)S5
S9         18   RD (unique items)
S10       727   S1(S)S2(S)S4
```

S11	290	S10(S)AUTHENTICAT?
S12	131	RD (unique items)
S13	25	S12 NOT PY=1999:2002

9/3,K/1 (Item 1 from file: 275)
DIALOG(R)File 275:Gale Group Computer DB(TM)

02408116 SUPPLIER NUMBER: 62653319 (USE FORMAT 7 OR 9 FOR FULL TEXT)
The Essential Guide to Installing Windows 2000 Server.(The Essential Guide to Installing Windows 2000 Server -- Windows 2000 Server is a sweet server indeed, once you get it installed. Our detailed guide will help you get it up and running with a minimum of fuss.)(Product Information)
Boyce, Jim
WinMag.com, NA
May 24, 2000
LANGUAGE: English RECORD TYPE: Fulltext; Abstract
WORD COUNT: 6468 LINE COUNT: 00496

TEXT:
...IP addresses of each server and note the address along with all other TCP/IP **configuration data** (DNS servers, and so on). For new servers, decide how you will allocate IP addresses...place a server between the Internet and the rest of your network. The server runs **firewall** or proxy software that helps insulate the LAN from the outside world. You might choose to implement a hardware-based **firewall** , security within your router hardware, or a combination for best security. In all cases, interfaces...
...for authentication. Finally, you'll need to acquire certificates if you intend to use Secure **Socket** Layer (**SSL**) on your Web servers, Layer Two **Tunneling** Protocol (L2TP) for **Virtual Private Network** (**VPN**) connections, or IP Security (IPSec) to secure traffic between computers. One of the easiest solutions...when TCP/IP is your only protocol -- in which case you should be using a **firewall** or proxy server for protection. (click image for expanded view) For security, unbind TCP/IP...giving you flexibility and security. If you need full remote-administration ability, consider using a **VPN** connection to the server for running the IIS console remotely. Those concerned about security on...

...set up the server for specific RRAS applications, such as Internet connection server, RAS server, **VPN** server, or network router. You can customize the settings as needed. If you prefer, you...

...what you can and cannot do with Remote Access. And Increasing Security on Windows 2000 **VPN** Server should be required reading for anyone responsible for the security relating to **VPN** connections. Post-install Tweaks You should perform several post-install tweaks on the server after ...Tools folder to create and modify user accounts and groups. You can use the Local **Security** Policy console to **configure** user rights and audit policies on the server and use the Domain **Security** Policy to **configure** domain-wide rights and audit policies. Tighten Security We've already mentioned one step in...

9/3,K/2 (Item 2 from file: 275)
DIALOG(R)File 275:Gale Group Computer DB(TM)

02344008 SUPPLIER NUMBER: 56744586 (USE FORMAT 7 OR 9 FOR FULL TEXT)
Find Your Own Comfort Level.(security and Web-to-host connectivity)(Internet/Web/Online Service Information)
McKendrick, Joseph
Enterprise Systems Journal, 14, 10, 20
Oct, 1999
ISSN: 1053-6566 LANGUAGE: English RECORD TYPE: Fulltext; Abstract
WORD COUNT: 961 LINE COUNT: 00080

...ABSTRACT: tier architectures underlying Web-to-host configurations have inherent security advantages. Security technologies such as **firewalls** , **SSL** transaction encryption, **VPNs** and digital certificates are discussed.

9/3,K/3 (Item 3 from file: 275)
DIALOG(R)File 275:Gale Group Computer DB(TM)

02329518 SUPPLIER NUMBER: 55705809 (USE FORMAT 7 OR 9 FOR FULL TEXT)
Aventail Makes Extranets Go. (Software Review) (Evaluation)
Young, Kevin
PC Week, 81
Sept 6, 1999
DOCUMENT TYPE: Evaluation ISSN: 0740-1604 LANGUAGE: English
RECORD TYPE: Fulltext; Abstract
WORD COUNT: 885 LINE COUNT: 00081

... stronger authentication and access control of the SSL/SOCKS combination.
However, a mixture of a **firewall** and IPSec **tunnels** that terminate at the **firewall** can come very close to providing the same level of access control and authentication. **SSL** /SOCKS operates slightly higher in the network stack, at the session layer as opposed to IPSec's network layer, allowing it to pass information such as IP and TCP **port numbers** and giving the **tunnel** end points extra **information** for making access-control decisions. SOCKS also has some **firewall** traversal capabilities.
Before implementing ExtraNet Center, administrators must consider their extranet topology demands. Aventail's...

9/3,K/4 (Item 4 from file: 275)
DIALOG(R)File 275:Gale Group Computer DB(TM)

02005320 SUPPLIER NUMBER: 18857716 (USE FORMAT 7 OR 9 FOR FULL TEXT)
Secure Windows to the Web. (Microsoft's Proxy Server) (Lab Note) (PC Week Netweek) (Software Review) (Evaluation)
Surkan, Michael
PC Week, v13, n45, pN1(2)
Nov 11, 1996
DOCUMENT TYPE: Evaluation ISSN: 0740-1604 LANGUAGE: English
RECORD TYPE: Fulltext; Abstract
WORD COUNT: 1155 LINE COUNT: 00096

...ABSTRACT: be modified via menus. However, the product lacks firewall features, support for event alerting and **virtual private networks** , and reverse proxy functions for redundancy and Web site performance purposes.

9/3,K/5 (Item 5 from file: 275)
DIALOG(R)File 275:Gale Group Computer DB(TM)

01871955 SUPPLIER NUMBER: 17819560 (USE FORMAT 7 OR 9 FOR FULL TEXT)
DEC ADDS RSA ENCRYPTION TO ITS INTERNET TUNNEL.
Computergram International, n805, pCGN12010013
Dec 1, 1995
ISSN: 0268-716X LANGUAGE: English RECORD TYPE: Fulltext
WORD COUNT: 626 LINE COUNT: 00053

... private data circuit and do not support end-to-end or trans-Internet privacy.
Firewall **tunnelling** prodcts require the use of their **tunnels** at both ends, since interoperability standards don't exist. DEC said its approach also wins out over Netscape's **SSL** Secure **Socket** Layer protocol, which also uses RSA encryption, since it is used at a different level of the IP stack. Secure **Socket** Layer encrypts **information** for applications, while **tunnels** establish a link for all connections between two networks. With Netscape applications the need to...

...must be modified to enable the request for an encrypted link. In

contrast, Digital Internet **tunnel** applications are not modified, and all the traffic between the **tunnels** is encrypted. The international version is due out this month and costs from $10,000...

9/3,K/6 (Item 1 from file: 621)
DIALOG(R)File 621:Gale Group New Prod.Annou.(R)

02664336 Supplier Number: 65634771 (USE FORMAT 7 FOR FULLTEXT)
Xcert Announces Sentry 4.5 PKI Software for Application Service Providers; Offers Easy-to-Deploy Security for Hosted Applications and Increased.
Business Wire, p2333
Oct 2, 2000
Language: English Record Type: Fulltext
Document Type: Newswire; Trade
Word Count: 558

... to protect their customers' interests as well as their own. Consequently, many ASPs are using **firewall** and intrusion detection methods to protect the perimeter of their data center operations, **VPNs** and authenticated **SSL sessions** to secure the **data** in transit in addition to passwords for authenticating user access to their hosted applications. "Despite...

...Xcert President and CEO. "Sentry 4.5 enables ASPs and AIPs to scale and manage **VPN** deployments by providing state-of-the-art key management services, that are a much higher...

9/3,K/7 (Item 1 from file: 636)
DIALOG(R)File 636:Gale Group Newsletter DB(TM)

04012336 Supplier Number: 53200015 (USE FORMAT 7 FOR FULLTEXT)
-MATRANET: MATRAnet presents M>Wall 4.0, the latest version of its high security firewall.
M2 Presswire, pNA
Nov 9, 1998
Language: English Record Type: Fulltext
Document Type: Newswire; Trade
Word Count: 1201

(USE FORMAT 7 FOR FULLTEXT)
TEXT:
...locally from any dedicated administrative computer on the network. Auditing and reporting tools continuously monitor **firewall** activity and report alarms in real time. User-level security and confidentiality M>Wall enables specific rights or restrictions to be assigned based on user profiles, simply by activating the **firewall** 's integrated authentication procedures. M>Wall provides strong authentication capabilities, which can be triggered for...

...simplifies user identification M>WallCard is the smartcard module of the M>Wall 4.0 **firewall** that ensures strong authentication. It enables users in a company to access information on their...

...in MATRAnet security and electronic business products. 168-bit triple-DES strong encryption for optimized **VPN** protection Seamless integration of M>Wall 4.0 with M> **Tunnel** provides strong encryption capabilities for **Virtual Private Networks** (**VPN**), enabling businesses to leverage the cost-efficiency benefits of the Internet in complete security. Drawing on Matra's extensive expertise and experience, M> **Tunnel** was developed in complete accordance with the IPSEC Internet security protocol. It uses 56 to 168-bit keys (DES, Triple DES) to provide strong cryptographic capability. In October 1997, M> **Tunnel** received approval from the French government agency for encryption regulations (SCSSI). Price: Starting at GBP...

...up to 50 users Availability: November 98 Technical characteristics Proxies and services supported: Web HTTP, **SSL** , Gopher Email

9/3,K/8 (Item 1 from file: 16)
DIALOG(R)File 16:Gale Group PROMT(R)

05591858 Supplier Number: 48464235 (USE FORMAT 7 FOR FULLTEXT)
Networking Chips -- Supports Compression, Data Encryption And User Authentication -- Volume shipment begins for Hi/fn encryption processor
Wirbel, Loring
Electronic Engineering Times, p98
May 4, 1998
Language: English Record Type: Fulltext
Document Type: Magazine/Journal; Trade
Word Count: 396

... both MD5 and Secure Hash Algorithm-1.
Data tunneling supported
The 7711 helps set up **data tunneling** for use in internal security or external **tunnels** to a corporate **firewall** . The device can work with the secure Internet Protocol extensions (IPsec), as well as with the Point-to-Point **Tunneling** Protocol, Layer 2 **Tunneling** Protocol, Secure **Sockets** Layer and Point-to-Point Protocol.
Hi/fn plans to leverage its recent acquisition of...

9/3,K/9 (Item 1 from file: 15)
DIALOG(R)File 15:ABI/Inform(R)

01748022 03-99012
The changing face of messaging
Kjaervik, Solveig Midtkandal
Telecommunications (International Edition) v32n12 PP: 61-62 Dec 1998
ISSN: 0040-2494 JRNL CODE: TIE
WORD COUNT: 1622

...TEXT: email and voice messaging as safe, if not even safer than other means of communication. **SSL** (secure **socket** layer) for example, is a widespread encrypting mechanism which encrypts communications between clients and servers. Until now, web servers have used **SSL** on a large scale, and there is a growing tendency for mail servers to use it. While the **SSL** protocol only encrypts messages between client and servers, PGP (pretty good privacy) and S/MIME...

... have access to the public keys of all the receivers. Many ISPs can now deliver **virtual private networks** (**VPNs**) over the Internet, an outsourced service ideal for companies with a geographical spread of business...

... s IP network, and secure clients at the smaller branches. A personal, secure, encrypted IP **tunnel** protects **information** going over the Internet. The ISP takes care of all investment costs regarding infrastructure and maintenance of lines, modem pools, **firewalls** etc.

ISP Messaging Architecture

Most of today's ISPs have mail servers based on 'sendmail...

9/3,K/10 (Item 1 from file: 647)
DIALOG(R)File 647:CMP Computer Fulltext

01160423 CMP ACCESSION NUMBER: EET19980504S0129

Networking Chips - Supports Compression, Data Encryption And User Authentication - Volume shipment begins for Hi/fn encryption processor
Loring Wirbel
ELECTRONIC ENGINEERING TIMES, 1998, n 1005, PG98
PUBLICATION DATE: 980504
JOURNAL CODE: EET LANGUAGE: English
RECORD TYPE: Fulltext
SECTION HEADING: Design
WORD COUNT: 394

... both MD5 and Secure Hash Algorithm-1.

Data tunneling supported

The 7711 helps set up **data tunneling** for use in internal security or external **tunnels** to a corporate **firewall** . The device can work with the secure Internet Protocol extensions (IPsec), as well as with the Point-to-Point **Tunneling** Protocol, Layer 2 **Tunneling** Protocol, Secure **Sockets** Layer and Point-to-Point Protocol.

Hi/fn plans to leverage its recent acquisition of...

9/3,K/11 (Item 1 from file: 674)
DIALOG(R)File 674:Computer News Fulltext

098623
Remote access receives a boost
Netilla Virtual Office offers an easy way to access network applications and data over the Web.
Byline: BY PAUL FERRILL
Journal: Network World Page Number: 19
Publication Date: January 14, 2002
Word Count: 740 Line Count: 68

Text:
... up the list of priorities for many network managers. Traditional products - including remote dial-up, **VPNs** and dedicated WANs - don't cut it because of high cost and slow speeds. Turnkey...

... works with Terminal Server function over the Web. All network traffic uses 128-bit Secure **Sockets** Layer security for maximum protection. User authentication is handled on a pass-through basis to...

... DNS has been configured properly and that the box can be seen from outside the **firewall** . You must install Windows 2000 Terminal Server on the server that hosts the applications, and...
... whether to flush the application password cache when launching applications. Administering applications is a breeze. **Information** needed to **configure** an application is stored in the directory on the server along with the executable file...

9/3,K/12 (Item 2 from file: 674)
DIALOG(R)File 674:Computer News Fulltext

098126
SonicWall adds speed, drops prices
Byline: Tim Greene
Journal: Network World
Publication Date: December 10, 2001
Word Count: 464 Line Count: 42

Text:
...www.sonicwall.com) Monday announced it is boosting the processing power of most of its **VPN** gear, significantly increasing their encryption speed.

At the same time, the company said it is...

... larger customers with more complex networks. Additionally, the company issued a new version of its **SSL** accelerator card software that enables the cards to handle more **SSL** sessions than before. The new software caches **information** about **sessions** that are still active but that are passing no data at the moment. This caching increases to 5,000 the number of concurrent **SSL** sessions the hardware supports. Caching also keeps processing and memory free to handle up to...

... latest release of SonicWall Global Management System software gives users a view of the entire **VPN** as well as high-level reporting on network performance. It also provides a tabular view of **firewall** activity and supports anti-virus installations at up to 1,000 nodes. "SonicWall has really...

9/3,K/13 (Item 3 from file: 674)
DIALOG(R)File 674:Computer News Fulltext

097117
Windows XP
New desktop operating system gets high marks for reliability, a new interface and improved multimedia features, but changes in the networking stack raise security issues.
Byline: By Tom Henderson, Network World Global Test Alliance
Journal: Network World Page Number: 49
Publication Date: October 29, 2001
Word Count: 1185 Line Count: 115

Text:
... of 2002. The Home Edition lacks enterprise functionality including tiered authentication services, IP Security (IPSec) **VPN** support, endemic file/folder encryption support and back-up software. Microsoft has imposed limitations on...

... Win 2000. The new Resultant Set of Policy utility gives you on-the-spot policy **configuration information** about any PC or logged-on user and can help you to debug policies for...

...with important exceptions noted below. Unlike its predecessor, XP allows applications nonroot, raw TCP/IP **sockets** access. This unprecedented access lets applications tap into the **Winsock** API (which controls network communications among other tasks) without control of the operating system kernel...

... is more pronounced in older and/or slower PCs.The downside is that nonroot raw **sockets** access also means that XP workstations, once infected with aggressive or hostile code in the...

... zombies, etc., could wreak havoc on network segments, as applications can gain control of the **Winsock** API stack autonomously and unauthenticated. In some cases, that's possible in current Windows versions but it's more difficult natively as raw **socket** capability can be installed through third- party tool kits - potentially letting hostile code to gain control. Most networked PCs haven't used nonroot raw **sockets** before because they haven't needed them. Microsoft apparently felt that improved performance was needed...

... But it places a certain burden on network professionals overseeing XP deployments to have integral **firewall** protections in place. Microsoft includes one, called the Internet Connection **Firewall** , which can be used on LANs, **VPNs** or dial-up connections to remote access servers or ISPs. However, we noted that Internet Connection **Firewall** affected Ethernet performance in some cases. We noticed this effect on machines that meet the ...SirCam Virus patch, but otherwise survived our Internet Security Systems RealSecure Scanner testing of the **firewall** and other port probes. The

firewall includes network address translation that didn't render the IPSec **VPN** protocol unusable as other personal **firewall** products can. XP also supports Session Initiation Protocol, an enabler for IP telephony and directory...

... life cycle and compatibility, and the potential danger from raw access to the TCP/IP **sockets** . A final consideration is that getting too far behind the current Windows revision demands an...

9/3,K/14 (Item 4 from file: 674)
DIALOG(R)File 674:Computer News Fulltext

097114
ABCs of videoconferencing
Pick the right client device, figure out LAN bandwidth requirements, nail down WAN links, then start conferencing.
Byline: Christine Perey
Journal: Network World Page Number: 46
Publication Date: October 29, 2001
Word Count: 2048 Line Count: 195

Text:
... signaling. The H.323 protocol does not require that two or more endpoints in a **session** send the same **data** rate they receive. A low-powered endpoint may only be able to encode at a management (an important issue when clients are set up behind a **firewall** and use network address translation), set performance metrics on a per-device or user basis ...

... other challenges remain. One of the biggest obstacles is getting real-time video traffic through **firewalls** . Since H.323-compliant applications use dynamically allocated **sockets** for audio, video and data channels, a **firewall** must be able to allow H.323 traffic through on an intelligent basis. The **firewall** must be either H.323-enabled with an H.323 proxy, or able to OsnoopO on the control channel to determine which dynamic **sockets** are in use for H.323 sessions, and to allow traffic through only as long one hour will generate nearly 1.4G bits of bandwidth. On a **VPN** the network usage costs are already fixed and the company will incur no additional charges...

9/3,K/15 (Item 5 from file: 674)
DIALOG(R)File 674:Computer News Fulltext

092730
Nokia adds to its VPN appliances
New boxes are custom fit to the size of branch office.
Byline: TIM GREENE
Journal: Network World
Publication Date: March 29, 2001
Word Count: 532 Line Count: 49

Text:
Enterprise customers looking to rapidly deploy a single inexpensive box to extend **firewall** and **VPN** protection to small offices now have new options from Nokia.Nokia this month will ship three new members of its IP line of Internet **VPN** appliances, two for 10- to 15-user offices, the IP51 and IP55, and one for...

... sites. The company also is introducing acceleration devices to off-load the processing of Secure **Sockets** Layer security with the idea of speeding up the e-commerce transactions that **SSL** is often used to protect. The combination **firewall** / **VPN** appliances are meant to simplify setting up **VPNs** . Rather than installing **VPN** and **firewall** software on a router or server at each site, companies can ship these boxes fully...

... Nokia with holding a lead in sales of these appliances, which are also made by **VPN** specialist vendors such as NetScreen and WatchGuard and network giants Cisco and Nortel.All three devices provide a **firewall** to protect the Internet access links at branch offices and establish IP Security-based, encrypted **tunnels** to other corporate sites. To handle this, Nokia adds Check Point **Firewall - VPN** -1 software to its dedicated **VPN** hardware.The IP51 is designed to sit between a WAN router and the branch-office...

... the router, two to LAN devices and one to corporate devices that are outside the **firewall** , such as Web servers, Nokia says. The IP530's **firewall** supports 50M-bit/sec throughput, and the device can encrypt using Triple-DES encryption at...

...weren't going to protect a $50-a-month DSL connection with a $30,000 **firewall** . With this type of device you don't have to make these Solomon-like decisions," says John Lawler, an analyst with Infonetics.To achieve this **firewall** speed, the IP530 uses a new feature of Check Point's software called Secure XL...

... president and general manager of Nokia's Internet devices division (see story, page XX). The **firewall** checks the source and type of traffic of each packet up to Layer 7 of the Open Systems Interconnection model until it **identifies** TCP/IP **sessions** that are authorized to pass through. It then updates a connection table that can screen subsequent packets by parsing them only to Layer 3, McDonald says. That can make the **firewall** three times faster using the same hardware, he says.The IP55 costs $1,295, the...

... 895 and the IP530 costs $16,995.Nokia also recently introduced Nokia CA200 and CA600 **SSL** accelerators. These devices handle **SSL** -processing Web servers, improving the transaction speed of **SSL** -protected sites. These devices employ clustering and load-balancing technology Nokia acquired with the purchase...

9/3,K/16 (Item 6 from file: 674)
DIALOG(R)File 674:Computer News Fulltext

092712
Nokia pumps up VPN appliances
Three new boxes target small to midsize offices and feature firewall support.
Journal: Network World Page Number: 17
Publication Date: April 02, 2001
Word Count: 519 Line Count: 48

Text:
nterprise customers looking to rapidly deploy a single inexpensive box to extend **firewall** and **VPN** protection to small offices now have new options from Nokia.Nokia will this month ship three new members of its IP line of Internet **VPN** appliances, two for 10- to 15-user offices, the IP51 and IP55, and one for...

... sites. The company also is introducing acceleration devices to off-load the processing of Secure **Sockets** Layer security with the idea of speeding up the e-commerce transactions that **SSL** is often used to protect. The combination **firewall** / **VPN** appliances are meant to simplify setting up **VPNs** . Rather than installing **VPN** and **firewall** software on a router or server at each site, companies can deploy these boxes fully...
... of IT staff, Nokia claims. Analysts say the new devices will help Nokia compete with **VPN** vendors such as NetScreen and WatchGuard and network giants Cisco and Nortel.All three devices provide a **firewall** to protect the Internet access links at branch offices and establish IP Security-based, encrypted **tunnels** to other corporate sites. To handle those functions, Nokia adds Check Point **Firewall - VPN** -1 software to its dedicated **VPN** hardware.The IP51 is designed to sit between a WAN router

and the branch-office...

... the router, two to LAN devices and one to corporate devices that are outside the **firewall** , such as Web servers, Nokia says. The IP530's **firewall** supports 50M bit/sec throughput, and the device can encrypt using Triple-DES encryption at...

...weren't going to protect a $50-a-month DSL connection with a $30,000 **firewall** . With this type of device you don't have to make these Solomon-like decisions," says John Lawler, an analyst with Infonetics.To achieve this **firewall** speed, the IP530 uses a new feature of Check Point's software called Secure XL, says Dan McDonald, vice president and general manager of Nokia's Internet devices division.The **firewall** checks the source and type of traffic of each packet up to Layer 7 of the Open Systems Interconnection model until it **identifies** TCP/IP **sessions** that are authorized to pass through. It then updates a connection table that can screen subsequent packets by parsing them only to Layer 3, McDonald says.That can make the **firewall** three times faster using the same hardware, he says.The IP55 costs $1,295, the...

...costs $895 and the IP530 costs $16,995.Nokia also introduced Nokia CA200 and CA600 **SSL** accelerators. These devices handle **SSL** -processing Web servers, improving the transaction speed of **SSL** -protected sites. These devices employ clustering and load-balancing technology Nokia acquired with the purchase...

9/3,K/17 (Item 7 from file: 674)
DIALOG(R)File 674:Computer News Fulltext

090006
A Xmas gift to send back
Byline: Mark Gibbs
Journal: Network World Page Number: 44
Publication Date: December 18, 2000
Word Count: 550 Line Count: 48

Text:
... discuss the source of this potential angst, let us fill in the background. You have **firewalls** in place for good reasons: to keep the bad guys out and, just as importantly, to control what your users can and cannot do.You've set up your **firewalls** to block instant messaging products, prevented access to e-mail servers other than corporate servers ...

...But just when you had it all sewn up along comes a product called HTTP-**Tunnel** to thwart you. Sorry.HTTP- **Tunnel** is a simple idea: Create a " **tunnel** " using a protocol (HTTP) that the **firewall** will allow and embed other protocols inside the **tunneling** protocol. Because the embedded protocol is hidden, the **firewall** has no idea that something unsanctioned is going on.At the other end of the **tunnel** there is a **tunnel** server that unwraps the embedded protocol and sends it to its destination. This is a...

...by now you should wonder how the application on the user's side of the **tunnel** knows the **tunnel** is there.There are three ways. The first works with applications that are aware of...

...the proxy on 127.0.0.1 (that's an alias for your local IP **address**) and **Port** 080. Once you start the HTTP- **Tunnel** client application, it will accept the SOCKS requests from the application and wrap the application's protocol inside HTTP requests.You must also be wondering what happens at the **tunnel** server end - it acts like the back end of a SOCKS server and modifies the request so the server is the source address. When the remote service responds, the **tunnel** server sends the reply packets to the real originating address and everyone is happy. Well...

...SocksCap32 has to launch the application for you as it fools around with the Windows **Sockets** layer and redirects the network I/O to the SOCKS server (in this case, the HTTP- **Tunnel** client). The third way is to use port mapping. This involves taking data received on the client side on a specific **socket** (such as address 127.0.0.1 and Port 110 for POP3 access) and mapping it explicitly to whichever server and port you specify.We tried HTTP- **Tunnel** and found that it's pretty easy to set up and doesn't seem to ...

9/3,K/18 (Item 8 from file: 674)
DIALOG(R)File 674:Computer News Fulltext

065092
Proprietary VPN is mixed bag
Product Review
InfoExpress virtual private network uses its own tunneling protocols
Byline: David M. Piscitello and Lisa A. Phifer
Journal: Computerworld Page Number: 52
Publication Date: March 09, 1998
Word Count: 660 Line Count: 66

Text:
Product Review InfoExpress Virtual TCP Secure Remote **VPN** Overall Grade: B InfoExpress, Inc. Los Altos, Calif. (650) 969-9609 www.infoexpress.com Price...

... per server; $89 per client Pros: Multiple session privacy levels Cons: No content filtering capabilities **Virtual private networks** (**VPN**) provide low-cost, remote access for telecommuters and mobile workers and secure wide-area links across the Internet among corporate facilities. The number of **VPNs** installed is still small, but **VPN** products are shipping, and vendors are establishing interoperability standards. The thing that is unusual about InfoExpress, Inc.'s InfoExpress Virtual TCP Secure Remote **VPN** is that it uses proprietary rather than standard protocols for **tunneling** . That is a mixed blessing. Users sacrifice interoperability but get nearly all the desired virtual network features in a single product set. Behind the **firewall** On the user end, client software forwards all communications through a gateway that establishes an encrypted connection across the Internet to another gateway, which sits behind a corporate **firewall** . The second gateway decrypts incoming data received over TCP, Telnet, or Secure **Sockets** Layer connections, authenticates users and controls their access to corporate servers. Virtual TCP software offers...

... products: encryption, strong authentication and authorization. It also has some features not always found in **virtual private network** software, including **session** level **data** compression and **VPN** support for Windows Internet Naming Service (WINS) -- a kind of domain name service for Windows...

... and support for WINS and MFS allows users to access shared file systems over a **VPN** **tunnel** . The product can authenticate users with third-party authentication servers or through a one-time...

... instructions for end users. After a few hiccups caused by spotty documentation and replacing the **winsock** .dll file, we successfully installed the client for systemwide **tunneling** and connected to a Virtual TCP gateway without customization. We automated the client to launch...

... key file. Scripting also can be used to launch dial-up networking connections prior to **tunneling** . Client software is the same for administration and operation, which raises the concern that users could modify administrator-supplied scripts and **configuration** . NO DOWNLOAD CONTROL The **security** administration module -- VTCP/Secure -- is a reasonably featured, stand-alone product that operates very much...

13/3,K/1 (Item 1 from file: 275)
DIALOG(R)File 275:Gale Group Computer DB(TM)

02233721 SUPPLIER NUMBER: 53131608
Stronghold of security -- SOCKS v5 promises enhanced security, butnot everyone agrees VPNs require its protection. (Internet/Web/Online Service Information)
Paone, Joe
LAN Times, 33(1)
Oct 26, 1998
ISSN: 1040-5917 LANGUAGE: English RECORD TYPE: Abstract

ABSTRACT: Secure **Sockets** (SOCKS) 5.0 is an IETF protocol standard that promises to improve security and access control on corporate networks. It provides user-based policy management, session-based security, improved **authentication** , standardized security on multimedia applications, and greater interoperability among compliant products. The new standard could ...

...on the existing version 4 by supporting multimedia UDP applications, user-based policy management and **authentication** ; SOCKS is already in widespread use as a **firewall** alternative, but has a low profile. Most see it as a fringe alternative to IPSec and PPTP for **VPNs** . IBM's eNetwork **Firewall** is the most prominent existing implementation, but market-leading **firewalls** do not support SOCKS 5 and are unlikely to offer it any time soon.

13/3,K/2 (Item 2 from file: 275)
DIALOG(R)File 275:Gale Group Computer DB(TM)

02155115 SUPPLIER NUMBER: 20417017 (USE FORMAT 7 OR 9 FOR FULL TEXT)
Now, That's a Secure VPN. (Aventail's Aventail VPN 2.5 virtual private network software) (Software Review) (Evaluation)
Phifer, Lisa A.
Windows Sources, v6, n4, p118(1)
April, 1998
DOCUMENT TYPE: Evaluation ISSN: 1065-9641 LANGUAGE: English
RECORD TYPE: Fulltext; Abstract
WORD COUNT: 1345 LINE COUNT: 00112

... To connect the server to the clients, we used a dual-Ethernet router.

Configuring the **VPN** server was quite similar to configuring a **firewall** or packet-filtering router, because you have to specify the security policy it should follow. First, we deployed the **VPN** server behind a packet-filtering router configured to deny incoming traffic to all hosts and ports except the default Socks port on the Aventail **VPN** server. For server **authentication** , we used **SSL** , and for client subauthentication, we chose CHAP (the popular Challenge Handshake **Authentication** Protocol many ISPs use) from the long list of supported methods, which include NT domains, RADIUS (Remote **Authentication** Dial-In User Services), and SecurID/ACE.

Then we implemented a security policy that permitted...

13/3,K/3 (Item 3 from file: 275)
DIALOG(R)File 275:Gale Group Computer DB(TM)

02153666 SUPPLIER NUMBER: 20426406
Securing E-commerce without heavy investments. (Internet/Web/Online Service Information)
Hartley, Bruce V.
Data Communications, v27, n4, p39(2)
March 21, 1998

ISSN: 0363-6399 LANGUAGE: English RECORD TYPE: Abstract

ABSTRACT: Many commercial products, including **firewalls** and Web servers, can be used to develop **virtual private networks** (**VPN**) for electronic commerce. Several security requirements are essential for electronic commerce systems. These include data confidentiality, secure connections and positive **authentication** . A conventional **firewall** can be extended to support data encryption, or a data encryption device can be added...

...each site. This approach requires a router port, DSU/CSU and a leased line. Secure **sockets** layer (**SSL**) connections are a solution for single transactions, such as credit card purchases. Other security technologies...

13/3,K/4 (Item 4 from file: 275)
DIALOG(R)File 275:Gale Group Computer DB(TM)
(c) 2002 The Gale Group. All rts. reserv.

02105234 SUPPLIER NUMBER: 19802218 (USE FORMAT 7 OR 9 FOR FULL TEXT)
VPN: Ascend Communications and Security Dynamics team up to deliver encrypted VPN starter package; Bundled package and value pricing create attractive VPN solution. (Company Business and Marketing)
EDGE: Work-Group Computing Report, v8, p22(1)
Sep 22, 1997
LANGUAGE: English RECORD TYPE: Fulltext
WORD COUNT: 1075 LINE COUNT: 00095

... encryption keys for the "virtual" remote population.
As remote users dial in, they must first **authenticate** themselves to the network using a SecurID token, which allows them to gain access to authorized resources on the enterprise. At that point, Ascend's **Firewall** Control Manager (FCM) determines whether a user is authorized to join a **VPN** . If so, the Secure Access Personal Edition software establishes a **tunnel** that extends to the dynamic **firewall** at the central site. Using Secure **Socket** Layer (**SSL**) technology which is based on RSA for key management and digital signatures, the FCM downloads an encryption key and a second **firewall** to the remote user's PC through that **tunnel** .
The encryption key allows the PC software to extend VPN access into the enterprise, while...

13/3,K/5 (Item 5 from file: 275)
DIALOG(R)File 275:Gale Group Computer DB(TM)
(c) 2002 The Gale Group. All rts. reserv.

02000686 SUPPLIER NUMBER: 18755004 (USE FORMAT 7 OR 9 FOR FULL TEXT)
Create a tough firewall. (network security) (Technology Information)
Wong, William
Network VAR, v4, n10, p35(4)
Oct, 1996
ISSN: 1082-8818 LANGUAGE: English RECORD TYPE: Fulltext; Abstract
WORD COUNT: 2399 LINE COUNT: 00198

... example, Terisa Systems' (Los Altos, CA) Secure HTTP (S-HTTP) provides a secure connection between **firewalls** , but only with applications using HTTP, not IP. The Secure **Sockets** Layer (**SSL**), being considered for a standard by the International Engineering Task Force (IETF), provides **authentication** , encryption, compression, and data integrity between applications (as does S-HTTP). Netscape Communications, (Mountain View, CA) Navigator supports **SSL** . It is possible to provide end-to-end protection at the IP or protocol level. This is called IP **tunneling** .
The most secure communications require two firewalls and encryption (see Figure 5). Proxy serve - application...

13/3,K/6 (Item 6 from file: 275)

DIALOG(R)File 275:Gale Group Computer DB(TM)
(c) 2002 The Gale Group. All rts. reserv.

01978866 SUPPLIER NUMBER: 18643719 (USE FORMAT 7 OR 9 FOR FULL TEXT)
FTP Software's OnNet32 2.0 easily provides the journeyman's tool kit.(Windows 95 TCP/IP Stack Wars) (PC Week Netweek) (Software Review)(Evaluation)
Phillips, Ken
PC Week, v13, n35, pN7(2)
Sep 2, 1996
DOCUMENT TYPE: Evaluation ISSN: 0740-1604 LANGUAGE: English
RECORD TYPE: Fulltext; Abstract
WORD COUNT: 682 LINE COUNT: 00059

...ABSTRACT: Sockets Layer (SSL) for secure financial transactions on the Web, NT domain security, firewalls and **virtual private networks** through the IP Security subset of IPv6 or CheckPoint Software Inc's **VPN** . The new version adds workflow automation, and the architecture has been changed to allow ActiveX...
... security side, OnNet32 also excels, supporting PGP (Pretty Good Privacy) for E-mail encryption and **authentication** , **SSL** (Secure **Sockets** Layer) for secure financial transactions on the World Wide Web, NT domain security, **firewalls** (SOCKS, ANS and Web Proxy), and **virtual private networks** via the IP Security subset of IPv6 or CheckPoint Software Inc.'s **VPN** .
Another new feature in OnNet32 Version 2.0 is workflow automation. FTP Software has altered...

13/3,K/7 (Item 1 from file: 621)
DIALOG(R)File 621:Gale Group New Prod.Annou.(R)
(c) 2002 The Gale Group. All rts. reserv.

01769750 Supplier Number: 53364768 (USE FORMAT 7 FOR FULLTEXT)
GemStone Systems Offers Industry's Most Comprehensive Implementation of Enterprise-Class Security in Enterprise Javabeans Application Server.
Business Wire, p0016
Dec 8, 1998
Language: English Record Type: Fulltext
Document Type: Newswire; Trade
Word Count: 1183

... developers to deliver secure communications solutions in conjunction with advanced application server technology."
GemStone/J **SSL** implementation supports a variety of encryption algorithms, key exchange systems, and **authentication** mechanisms that gives customers the best security technology available. Among those security features are encryption...

...RSA, DSS, DES and triple DES), key systems (Diffie-Hellman and El-Gamal) and certificate **authentication** mechanisms (MD5, SHA-1 and X.509). The **SSL** implementation also supports server and client **authentication** , session caching and **SSL** **tunneling** for **firewalls** .
"As our customers move into deployment, it is critical that over-the-wire security is...

13/3,K/8 (Item 2 from file: 621)
DIALOG(R)File 621:Gale Group New Prod.Annou.(R)
(c) 2002 The Gale Group. All rts. reserv.

01647034 Supplier Number: 48466266 (USE FORMAT 7 FOR FULLTEXT)
Aventail Dispels VPN Market Confusion at Networld+Interop '98 Las Vegas
PR Newswire, p0504SFM046
May 4, 1998
Language: English Record Type: Fulltext
Document Type: Newswire; Trade
Word Count: 659

... Internet, attendees can visit booth #1621 in the South Hall.
The latest version of Aventail **VPN** (TM) includes features such as intelligent **SSL** compression and Secure Enterprise Explorer(TM), a secure method of Windows file browsing. Aventail **VPN** is the only product with a full suite of **VPN** services beyond basic encryption, including pinpoint access controls, user-based **authentication** , key/certificate management and distribution, active content filtering, a non-intrusive client, and sophisticated management tools. Aventail **VPN** is also interoperable with any **firewall** including, Check Point's **Firewall** -1 (Nasdaq: CHKPF), Raptor Systems' (Nasdaq: AXNT) Eagle **Firewall** , and Network Associates' (Nasdaq: NETA) Gauntlet. In addition, Aventail **VPN** works with and adds value to **tunneling** protocols such as Microsoft's (Nasdaq: MSFT) Point to Point **Tunneling** Protocol (PPTP), IPSec, and Cisco's (Nasdaq: CSCO) Layer Two Forwarding (L2F).
About Aventail Corporation...

13/3,K/9 (Item 3 from file: 621)
DIALOG(R)File 621:Gale Group New Prod.Annou.(R)

01601391 Supplier Number: 48245567 (USE FORMAT 7 FOR FULLTEXT)
Differential Inc.'s FileDrive V1.5 Provides Extranet Developers With Faster, More Secure Large File Transfer Capabilities.
Business Wire, p01260164
Jan 26, 1998
Language: English Record Type: Fulltext
Document Type: Newswire; Trade
Word Count: 481

... FileDrive V1.5 also contains state-of-the-art open security standards, such as Secure **Sockets** Layer (**SSL**) Version3 encryption and X.509 digital certificates, for increased privacy and **authentication** . Seamless operation is assured through FileDrive's unique feature of adaptive **tunneling** through **firewalls** and proxyd, regardless of network outages or computer cFileDrive V1.5 is designed to support...

13/3,K/10 (Item 4 from file: 621)
DIALOG(R)File 621:Gale Group New Prod.Annou.(R)

01570100 Supplier Number: 47982996 (USE FORMAT 7 FOR FULLTEXT)
Ascend Communications and Security Dynamics Team Up to Deliver Encrypted VPN Starter Package; Bundled Package and Value Pricing Create Attractive VPN Solution.
Business Wire, p9160023
Sept 16, 1997
Language: English Record Type: Fulltext
Document Type: Newswire; Trade
Word Count: 816

... encryption keys for the "virtual" remote population.
As remote users dial in, they must first **authenticate** themselves to the network using a SecurID token, which allows them to gain access to authorized resources on the enterprise. At that point, Ascend's **Firewall** Control Manager (FCM) determines whether a user is authorized to join a **VPN** . If so, the Secure Access Personal Edition software establishes a **tunnel** that extends to the dynamic **firewall** at the central site. Using Secure **Socket** Layer (**SSL**) technology which is based on RSA for key management and digital signatures, the FCM downloads an encryption key and a second **firewall** to the remote user's PC through that **tunnel** .
The encryption key allows the PC software to extend VPN access into the enterprise, while...

13/3,K/11 (Item 1 from file: 636)

DIALOG(R)File 636:Gale Group Newsletter DB(TM)
(c) 2002 The Gale Group. All rts. reserv.

04012336 Supplier Number: 53200015 (USE FORMAT 7 FOR FULLTEXT)
-MATRANET: MATRAnet presents M>Wall 4.0, the latest version of its high security firewall.
M2 Presswire, pNA
Nov 9, 1998
Language: English Record Type: Fulltext
Document Type: Newswire; Trade
Word Count: 1201

(USE FORMAT 7 FOR FULLTEXT)
TEXT:
...1998-MATRANET: MATRAnet presents M>Wall 4.0, the latest version of its high security **firewall** (C)1994-98 M2 COMMUNICATIONS LTD RDATE:061198 -- Tighter security for the end-user and simplified network administration MATRAnet today announced version 4 of M>Wall, its high-level security **firewall** . M>Wall 4.0 provides a Java-based user-friendly administration interface, enabling the remote administration of multiple **firewalls** . In addition, M>Wall 4 supports smartcard **authentication** and incorporates extended capabilities for the strong **authentication** of POP3 and SMTP email protocols. It employs LDAP directories and Radius identification servers to manage **authenticated** users. Finally, M>Wall 4 includes a 168-bit triple-DES strong encryption module for...

...a seamless Internet Security Strategy, built around the high-level security M>Wall 4.0 **firewall** , with add-ons to meet specific needs. Five levels of protection for incoming and outgoing...

...based inspection -- inspection of data flows right up to the application level, for every communication. * **Authentication** : the M>Wall Card module enables user identification with a smartcard. * Encryption -- scrambling of information...

...locally from any dedicated administrative computer on the network. Auditing and reporting tools continuously monitor **firewall** activity and report alarms in real time. User-level security and confidentiality M>Wall enables specific rights or restrictions to be assigned based on user profiles, simply by activating the **firewall** 's integrated **authentication** procedures. M>Wall provides strong **authentication** capabilities, which can be triggered for all TCP-type protocols, such as HTTP, FTP, Telnet, SMTP, POP 3, etc. M>Wall supports a wide range of **authentication** tokens, including MATRAnet's M>WallKey and M>WallCard smartcard modules, together with a dozen...
...Defender, Digipass or Vasco. M>Wall is also compatible with LDAP and RADIUS type user **authentication** databases. Smartcard solution simplifies user identification M>WallCard is the smartcard module of the M>Wall 4.0 **firewall** that ensures strong **authentication** . It enables users in a company to access information on their intranet or on the Extranet using a personal smartcard containing their user ID. Smartcard **authentication** provides a very deep level of security and integrity in a convenient, standard and customizable...

...in MATRAnet security and electronic business products. 168-bit triple-DES strong encryption for optimized **VPN** protection Seamless integration of M>Wall 4.0 with M> **Tunnel** provides strong encryption capabilities for **Virtual Private Networks** (**VPN**), enabling businesses to leverage the cost-efficiency benefits of the Internet in complete security. Drawing on Matra's extensive expertise and experience, M> **Tunnel** was developed in complete accordance with the IPSEC Internet security protocol. It uses 56 to 168-bit keys (DES, Triple DES) to provide strong cryptographic capability. In October 1997, M> **Tunnel** received approval from the French government agency for encryption regulations (SCSSI). Price: Starting at GBP...

...up to 50 users Availability: November 98 Technical characteristics Proxies and services supported: Web HTTP, **SSL** , Gopher Email

13/3,K/12 (Item 2 from file: 636)
DIALOG(R)File 636:Gale Group Newsletter DB(TM)

03700159 Supplier Number: 47985274 (USE FORMAT 7 FOR FULLTEXT)
ASCEND: Ascend and Security Dynamics team up to deliver Encrypted VPN Starter Package
M2 Presswire, pN/A
Sept 17, 1997
Language: English Record Type: Fulltext
Document Type: Newswire; Trade
Word Count: 1310

... encryption keys for the "virtual" remote population.
As remote users dial in, they must first **authenticate** themselves to the network using a SecurID token, which allows them to gain access to authorized resources on the enterprise. At that point, Ascend's **Firewall** Control Manager (FCM) determines whether a user is authorized to join a **VPN** . If so, the Secure Access Personal Edition software establishes a **tunnel** that extends to the dynamic **firewall** at the central site. Using Secure **Socket** Layer (**SSL**) technology which is based on RSA for key management and digital signatures, the FCM downloads an encryption key and a second **firewall** to the remote user's PC through that **tunnel** . The encryption key allows the PC software to extend **VPN** access into the enterprise, while the **firewall** blocks far-end entry to the **tunnel** . This double layer of **firewalls** is an important precaution. With the second **firewall** in place, intruders will be unable to enter the **tunnel** should the remote user decide to browse the Internet while the **VPN** is in session.
"This is the perfect package for an organization, such as ours, whose ...

13/3,K/13 (Item 1 from file: 16)
DIALOG(R)File 16:Gale Group PROMT(R)

07059746 Supplier Number: 59271298 (USE FORMAT 7 FOR FULLTEXT)
Gentlemen, Start Your VPN Engines!(Company Business and Marketing)
LEFEVRE, JIM
ENT, v2, n16, p28
Oct 22, 1997
Language: English Record Type: Fulltext
Document Type: Magazine/Journal; Professional
Word Count: 622

... software, which automatically generates firewall objects and encryption keys for remote users.
Remote users must **authenticate** themselves with a SecurID token. Once a user is **authenticated** , Ascend's FCM software determines whether the user is able to join a **VPN** . If so, Ascend's Secure Access Personal Edition client software establishes a **tunnel** to the **firewall** at the central site, and FCM downloads an encryption key and a second **firewall** to the remote user through the **tunnel** . RSAs Secure **Sockets** Layer (**SSL**) technology is employed to make certain the key and the **firewall** arrive safely. The key enables the user to access the enterprise resources, and the second **firewall** prevents other users from entering the **tunnel** , adding another layer of security.
The Encrypted VPN Starter Kit is expected to be available...

13/3,K/14 (Item 2 from file: 16)
DIALOG(R)File 16:Gale Group PROMT(R)

06058765 Supplier Number: 54841573 (USE FORMAT 7 FOR FULLTEXT)

LAN-to-LAN VPNs: Secure Enough?(virtual private network)(Technology Information)
Steinke, Steve
Network, pNA
August 1, 1998
Language: English Record Type: Fulltext Abstract
Document Type: Magazine/Journal; Trade
Word Count: 4249

... are often called Session-layer operations.)
Transport Layer Security (TLS), formerly known as the Secure **Sockets** Layer (**SSL**), is often used to provide encryption from the **tunnel** initiator to the **tunnel** terminator. The IETF has defined a protocol known as SOCKS to standardize **authenticated firewall** traversal, and SOCKS 5 is currently the standards-based way to implement circuit proxies.
In a SOCKS 5 circuit proxy, a client computer establishes an **authenticated socket** (or session) with a server acting as a proxy; the proxy is the only way to get through the **firewall** . The proxy, in turn, conducts any operations requested by the client. Because the proxy is aware of traffic at the **socket** level, it can apply highly-granular controls, such as blocking specific applications to users without the right privileges. By comparison, layer-2 and layer-3 **VPNs** basically turn the spigot on for all traffic over an **authenticated tunnel** , which may be a problem if the network at the other end of the **tunnel** is not fully trusted.
Circuit-proxy VPNs, like IPSec, are IP-specific. However, where IPSec ...

13/3,K/15 (Item 3 from file: 16)
DIALOG(R)File 16:Gale Group PROMT(R)
(c) 2002 The Gale Group. All rts. reserv.

04544735 Supplier Number: 46678798 (USE FORMAT 7 FOR FULLTEXT)
FTP Software's OnNet32 2.0 easily provides the journeyman's tool kit
PC Week, pN07
Sept 2, 1996
Language: English Record Type: Fulltext
Document Type: Magazine/Journal; Tabloid; General Trade
Word Count: 642

... security side, OnNet32 also excels, supporting PGP (Pretty Good Privacy) for E-mail encryption and **authentication** , **SSL** (Secure **Sockets** Layer) for secure financial transactions on the World Wide Web, NT domain security, **firewalls** (SOCKS, ANS and Web Proxy), and **virtual private networks** via the IP Security subset of IPv6 or CheckPoint Software Inc.'s **VPN** .
Another new feature in OnNet32 Version 2.0 is workflow automation. FTP Software has altered...

13/3,K/16 (Item 4 from file: 16)
DIALOG(R)File 16:Gale Group PROMT(R)
(c) 2002 The Gale Group. All rts. reserv.

04456936 Supplier Number: 46542770 (USE FORMAT 7 FOR FULLTEXT)
FTP Software's OrtNer32 v2.0 Raises the Bar on TCP/IP Connectivity by Delivering Five Industry "Firsts"
News Release, pN/A
July 15, 1996
Language: English Record Type: Fulltext
Document Type: Magazine/Journal; Trade
Word Count: 1099

(USE FORMAT 7 FOR FULLTEXT)
TEXT:
...generation IP, IPv6, offering enterprises the benefits of the kernel's additional sealability and security; * **WinSock** 2.0, ensuring full 32-bit

interoperability with other **WinSock** applications; * IPSECurity security standards; * **Virtual Private Network** security standards. FTP Software's OnNet32 v2.0 enables network administrators to centrally install, configure...

...infrastructure for tomorrow's networks today. With the industry's first support for IPv6 and **WinSock** 2.0, OnNet32 v2.0 provides a forward planning foundation that protects an organization's...
...including support for IPSECurity, which provides point-to-point security based on open standards for **authentication** and encryption. OnNet32 v2.0 also includes one of the first product implementations of PGP...

...send an encrypted message with a single mouse click. As the first suite to support **VPN** (**Virtual Private Network**), in addition to SOCKS and ANS **firewalls** , OnNet32 v2.0 gives administrators the tools they need to control how network applications can navigate between **firewalls** . "We are always pleased with the power and utility FTP Software adds to the TCP...

13/3,K/17 (Item 1 from file: 148)
DIALOG(R)File 148:Gale Group Trade & Industry DB
(c)2002 The Gale Group. All rts. reserv.

09770893 SUPPLIER NUMBER: 19827589 (USE FORMAT 7 OR 9 FOR FULL TEXT)
Aventail Joins Value Chain Initiative and Ships First Supply-Chain VPN Solution
PR Newswire, p1006SFM104
Oct 6, 1997
LANGUAGE: English RECORD TYPE: Fulltext
WORD COUNT: 895 LINE COUNT: 00084

... TCP and most UDP clients and custom corporate applications.
Built on a flexible architecture. Aventail **VPN** supports multiple **authentication** and encryption methods including: CHAP, RADIUS, SecurID, **SSL** , DES, MD4, MD5, SHA-1, and RC4. In addition, Aventail **VPN** is the only **VPN** solution that is compatible with all **firewalls** and **tunneling** protocols, such as Microsoft's Point to Point **Tunneling** Protocol (PPTP) and Cisco's Layer Two Forwarding (L2F).
Building a Hiqhly-Secure Supply-Chain...

13/3,K/18 (Item 2 from file: 148)
DIALOG(R)File 148:Gale Group Trade & Industry DB
(c)2002 The Gale Group. All rts. reserv.

09728631 SUPPLIER NUMBER: 19756178 (USE FORMAT 7 OR 9 FOR FULL TEXT)
Security Advisor Magazine - Advisor Publications Announces Security Advisor.
Business Wire, p9120176
Sep 12, 1997
LANGUAGE: English RECORD TYPE: Fulltext
WORD COUNT: 634 LINE COUNT: 00061

... articles, case studies, tips, answers to reader questions, and comprehensive product information.
Security topics include **authentication** , encryption, **firewalls** , viruses, routers, passwords, Intranets, year 2000, LANs, databases, applications, components and applets, communications devices and networks, certificates, WANs, servers, the Internet and World Wide Web, **tunneling** , systems management, Extranets, **virtual private networks** , scripts, **SSL** , Java and more.
With so many ways to breach or damage an NT or network...

13/3,K/19 (Item 1 from file: 15)
DIALOG(R)File 15:ABI/Inform(R)
(c) 2002 ProQuest Info&Learning. All rts. reserv.

01380285 00-31272
Tunneling is key to secure extranets
Kobielus, James
Network World v14n9 PP: 35 Mar 3, 1997
ISSN: 0887-7661 JRNL CODE: NWW
WORD COUNT: 730

...TEXT: volumes on your extranet increase, you'll need such value-added security features as protocol **tunneling** , public-key certificates and **authentication** tokens. You may have already acquired these technologies for intranet and remote access applications, thereby...

... ingredients needed to implement a basic extranet, including legacy applications, Web servers, intranets, proxy servers, **firewalls** , Internet service providers and Secure **Sockets** Layer-capable browsers.

Perhaps the most important security technology for extranets is protocol tunneling. Tunneling...

13/3,K/20 (Item 1 from file: 9)
DIALOG(R)File 9:Business & Industry(R)

01672983
Network Security Built On Simple Standards
(Aventail Corp is offering a firewall with the SOCKs socket protocol and the Secure Sockets Layer (SSL))
Interactive Week, v 3, n 26, p 48
November 18, 1996
DOCUMENT TYPE: Journal ISSN: 1078-7259 (United States)
LANGUAGE: English RECORD TYPE: Abstract

ABSTRACT:
Aventail Corp is offering a **firewall** with the SOCKs **socket** protocol and the Secure **Sockets** Layer (**SSL**), which offer **authentication** and encryption of applications and data that move across computer networks. The firm is promoting...

...SOCKs to router vendors and Internet service providers (ISPs) who want to offer support for **virtual private networking** , secure Internet links between users and a service provider and between users and corporate networks...

13/3,K/21 (Item 1 from file: 647)
DIALOG(R)File 647:CMP Computer Fulltext

01176680 CMP ACCESSION NUMBER: LAN19981026S0019
Stronghold of security - SOCKS v5 promises enhanced security, but not everyone agrees VPNs require its protection (Virtual Private Networks)
Joe Paone
LAN TIMES, 1998, n 1522, PG33
PUBLICATION DATE: 981026
JOURNAL CODE: LAN LANGUAGE: English
RECORD TYPE: Fulltext
SECTION HEADING: Wide Area
WORD COUNT: 1257

Hence, welcome a new champion to the fortifications of **firewalls** , **VPN tunnels** , **authentication** servers, and encryption algorithms protecting your network: Secure **Sockets** (SOCKS) version 5.

The IETF protocol promises to bring a number of security and access ...

13/3,K/22 (Item 1 from file: 674)
DIALOG(R)File 674:Computer News Fulltext

070143
HP widens security reach with firewall, VPN deals
Byline: Ellen Messmer
Journal: Network World
Publication Date: November 05, 1998
Word Count: 324 Line Count: 30

Text:
...Hewlett-Packard says it will bolster its security line by reselling the Axent Technologies Raptor **firewall** and Aventail **virtual private network** gear.Axent, which gains an exclusive reseller deal with HP, will also work with HP...

... hardened" Web server called VirtualVault. According to, HP will be focusing exclusively on the Raptor **firewall** in its marketing efforts for the foreseeable future and has no plans to sell other brands of **firewalls** ."HP technical staff will have to have complete knowledge of the Raptor **firewall** ," said Roberto Medrano, general manager of HP's Internet Security Operation.With HP's vast sales and support channels here and abroad, the **firewall** re-sale deal promises to be a boon to Axent. The loser, though, may be Check Point Technologies, whose **Firewall** -1 product was under consideration at one point by HP as well. Axent's strong...

...come in via common gateway interface scripts. Medrano said he expects to see the Raptor **firewall** and VirtualVault more closely integrated in the future so that the two products can share...

... that would assist in warding off hackers.Under the deal to re-sell the Aventail **VPN** , HP is rounding out a security portfolio with a client/server software product that uses the Secure **Sockets** Layer (**SSL**) and the SOCKS v.5 protocols to **authenticate** users and set up an encrypted session between IP-based applications.The Aventail **VPN** supports HP-UX, Windows NT, Sun Solaris, AIX, BSDI, Digital Unix, and Linux, and will...

13/3,K/23 (Item 2 from file: 674)
DIALOG(R)File 674:Computer News Fulltext

065092
Proprietary VPN is mixed bag
Product Review
InfoExpress virtual private network uses its own tunneling protocols
Byline: David M. Piscitello and Lisa A. Phifer
Journal: Computerworld Page Number: 52
Publication Date: March 09, 1998
Word Count: 660 Line Count: 66

Text:
Product Review InfoExpress Virtual TCP Secure Remote **VPN** Overall Grade: B InfoExpress, Inc. Los Altos, Calif. (650) 969-9609 www.infoexpress.com Price...

... per server; $89 per client Pros: Multiple session privacy levels Cons: No content filtering capabilities **Virtual private networks** (**VPN**) provide low-cost, remote access for telecommuters and mobile workers and secure wide-area links across the Internet among corporate facilities. The number of **VPNs** installed is still small, but **VPN** products are shipping, and vendors are establishing interoperability standards. The thing that is unusual about InfoExpress, Inc.'s InfoExpress Virtual TCP Secure Remote **VPN** is that it uses proprietary rather than standard protocols for **tunneling** . That is a mixed blessing. Users sacrifice interoperability but get nearly all the desired virtual network features in a single product

set. Behind the **firewall** On the user end, client software forwards all communications through a gateway that establishes an encrypted connection across the Internet to another gateway, which sits behind a corporate **firewall** . The second gateway decrypts incoming data received over TCP, Telnet, or Secure **Sockets** Layer connections, **authenticates** users and controls their access to corporate servers. Virtual TCP software offers features that administrators have come to expect from secure remote-access products: encryption, strong **authentication** and authorization. It also has some features not always found in **virtual private network** software, including session level data compression and **VPN** support for Windows Internet Naming Service (WINS) -- a kind of domain name service for Windows...

... and support for WINS and MFS allows users to access shared file systems over a **VPN tunnel** . The product can **authenticate** users with third-party **authentication** servers or through a one-time password system built in to the product's gateway...

... instructions for end users. After a few hiccups caused by spotty documentation and replacing the **winsock** .dll file, we successfully installed the client for systemwide **tunneling** and connected to a Virtual TCP gateway without customization. We automated the client to launch...

... key file. Scripting also can be used to launch dial-up networking connections prior to **tunneling** . Client software is the same for administration and operation, which raises the concern that users...

13/3,K/24 (Item 1 from file: 813)
DIALOG(R)File 813:PR Newswire

1213276 SFM052
DataChannel Enhances Extranet Strategy With Aventail Solution

DATE: January 19, 1998 14:23 EST WORD COUNT: 844

CORRECTION:
... that the mention in the third paragraph of Aventail's product, referred to as a firewall **, is incorrect. Aventail** VPN **is a policy-based** Virtual Private Network **(VPN) software solution. Also, in the first bullet point following the fourth paragraph, when referencing** authentication **, SOCKS is not an** authentication **method. SOCKS is an IETF-approved security protocol standard which enables Aventail** VPN **to support multiple** authentication **methods including digital certificates, token-based** authentication **, CHAP, RADIUS,** SSL **, or username/password.**

SOURCE DataChannel, Inc.

13/3,K/25 (Item 2 from file: 813)
DIALOG(R)File 813:PR Newswire

1111959 CHM001
Frost & Sullivan Says Internet Helping Network Security Companies Protect Their Profits

DATE: June 16, 1997 08:04 EDT WORD COUNT: 1,358

... standard (DSS), electronic data interchange (EDI), electronic mail (E-mail), federal bureau of investigation (FBI), **firewall** , application level gateway, **authentication** , third party trusted host, kerberos, LANs, WANs, **virtual private network** (VP), certificate-based public key, file transfer protocol (FTP), generic security services (GSS), graphical user...

... Personal Identification Number (PIN), Public Key Infrastructure (PKI),

Physical Layer and Convergence Protocol (PLCP), Remote **Authentication** Dial In User Service (RADIUS), Rivest, Shamir, and Adelman (RSA), Security Administrator's Tool for...

... Simple Mail Transfer Protocol (SMTP), Secure Network Key (SNK), Small Office Home Office (SOHO), Secure **Sockets** Layers (**SSL**), Secure **Virtual Private Network** (SVPN), Terminal Access Controller Access Control System (TACACS), Transmission Control Protocol (TCP), Transmission Control Protocol...